MICRO FOCUS

Open Enterprise Server 2023

NSS AD Administration Guide

October 2022

Legal Notices

© Copyright 2022 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 7

1 Overview of NSS AD Support 9

1.1 Understanding What Changed to Enable NSS AD Support in OES . . . 9
1.1.1 OES CIFS Access Changes . . . 10
1.1.2 OES Service Changes For NSS AD . . . 11
1.1.3 Multi-Forest Support for AD Users . . . 11
1.1.4 Utility and Management Tool Changes . . . 12

2 What's New or Changed in NSS AD 13

2.1 What's New or Changed in NSS AD (OES 2023) . . . 13
2.1.1 OES User Rights Map (NURM) Utility . . . 13

3 Preparing to Deploy NSS AD 15

3.1 Software and Hardware Requirements . . . 15
3.2 Meeting NSS AD Infrastructure Requirements . . . 15
3.3 Joining OES to AD Domain When OES and AD are Present in Different DNS Domain . . . 17
3.4 Planning to Assign AD User and Group Trustee Rights . . . 17
3.5 Coexistence with NSS AD . . . 18
3.5.1 Incompatiblities at a Server Level . . . 18
3.5.2 NSS AD Is Network-Compatible with All OES Services . . . 18
3.5.3 NSS AD Doesn't Affect Backward Compatibility . . . 18
3.5.4 Ensuring DST Support for NSS AD . . . 19
3.5.5 DFS Deployment with NSS AD . . . 19
3.6 Caveats for Deploying NSS AD . . . 20
3.6.1 Clustered Node Issue . . . 20
3.6.2 Recommendations During Upgrade . . . 20
3.7 Joining OES to a DSfW Domain . . . 21
3.7.1 Accessing NSS Over CIFS by eDirectory User Set As DSfW Users . . . 21
3.7.2 Accessing NSS Over CIFS by eDirectory Users As DSfW Users and DSfW Domain Having a Trust With One or More AD Domains/Forests . . . 22

4 Installing and Configuring NSS AD Support 23

4.1 Installing a New OES Server and Deploying NSS AD . . . 24
4.2 Upgrading to OES 2018 SP2 and Deploying NSS AD (Non-Clustered Environment) . . . 32
4.3 Upgrading to OES 2018 SP2 and Deploying NSS AD (Clustered Environment) . . . 39
4.4 Leave a AD Domain . . . 45
4.5 Reconfiguring NSS AD . . . 46
4.6 Renaming the Netbios Name of OES Host or Cluster Resource . . . 47

5 Assigning NSS Trustee Rights for AD Users and Groups 49

5.1 Overview of the Provisioning Process . . . 49

5.2 NURM Provisioning Caveats 50
5.2.1 iManager Created NetIQ IDM Map Files Do Not Work with NURM 50
5.2.2 NURM eDirectory User Must Have a CIFS Universal Password Policy 50

6 Managing NSS AD 53

7 NSS AD Utilities and Tools 57

7.1 List of NSS AD Supported Tools 57
7.2 NIT (Novell Identity Translator) 58
7.2.1 A New NSS Authorization Model 59
7.2.2 Not All Users Have UIDs by Default 59
7.2.3 Ensuring that Your CIFS-NSS Users Have UIDs 59
7.2.4 Which OES Components Rely on NIT 60
7.2.5 What NIT Does 60
7.2.6 Prerequisites 61
7.2.7 NIT Components 61
7.2.8 NIT Log Files 61
7.2.9 Interactions With eDirectory and Active Directory 62
7.2.10 How NIT Works 62
7.2.11 Active Directory users: 63
7.2.12 eDirectory users: 63
7.2.13 Task FAQ 63
7.2.14 Administrative Access Restrictions 64
7.2.15 Performance and Tuning 65
7.3 novell-ad-util 65
7.3.1 novell-ad-util Command Line Utility 65
7.4 NURM (OES User Rights Map) 71
7.4.1 Prerequisites 71
7.4.2 Accessing OES User Rights Map Utility (NURM) 71
7.4.3 Mapping Users 72
7.4.4 Mapping Rights 75
7.4.5 Viewing Rights 76
7.4.6 Changing the NURM Settings 77
7.4.7 NURM Command Line Utility 78
7.5 NFARM (OES File Access Rights Management) 83
7.5.1 NFARM Support Matrix 85
7.5.2 Prerequisites for Installing NFARM 85
7.5.3 Installing and Accessing NFARM 86
7.5.4 Managing the Trustee Rights in the NSS File System 86
7.5.5 Information or Directory Quota 93
7.5.6 User Quota 93
7.5.7 File System Rights 95
7.5.8 Settings (Mac) 96
7.5.9 Salvage and Purge 96
7.5.10 Logs 97
7.6 FTP (Pure-FTPd) and OES for AD Users 97
7.6.1 Planning for Pure-FTPd 97
7.6.2 Installing Pure-FTPd 97
7.6.3 Home Directory Support in Pure-FTPd 98
7.6.4 Prerequisites 99
7.6.5 Configuring Pure-FTPd on an OES Server 99
7.6.6 Administering and Managing Pure-FTPd on an OES Server 99
7.6.7 SMB Access for AD Users 102

7.6.8 Limitations 102

8 Troubleshooting 105

8.1 OES Storage Services AD Configuration is Greyed Out 105
8.2 Domain Leave Fails Using the novell-ad-util 105
8.3 Verification of the Container Object Fails During the AD Domain Join Process 106
8.4 Troubleshooting NFARM on MAC 106
8.4.1 'Rights Management' Menu Not Available 106
8.4.2 Unable to view Trustees in the Trustee Rights or User Quotas Tab 106
8.4.3 Connection to Active Directory Failed 106
8.4.4 NFARM Terminated Unexpectedly 107
8.5 Troubleshooting NURM 107
8.5.1 Unable to Map eDirectory Users in NURM 107
8.5.2 Volumes are not Listed in the View Rights and Map Rights Pages 108
8.5.3 Active Directory User Names With Special Characters are Ignored 108
8.5.4 View Rights Option Does Not Work in NURM When There are 200K Users 108
8.6 Troubleshooting NIT 108

A Reference Information 111

A.1 NIT Error Codes 111

About This Guide

This documentation describes how to install, deploy, and administer the NSS AD service included with OES 2023.

- Chapter 1, “Overview of NSS AD Support,” on page 9
- Chapter 2, “What’s New or Changed in NSS AD,” on page 13
- Chapter 3, “Preparing to Deploy NSS AD,” on page 15
- Chapter 4, “Installing and Configuring NSS AD Support,” on page 23
- Chapter 5, “Assigning NSS Trustee Rights for AD Users and Groups,” on page 49
- Chapter 6, “Managing NSS AD,” on page 53
- Chapter 7, “NSS AD Utilities and Tools,” on page 57
- Chapter 8, “Troubleshooting,” on page 105
- Appendix A, “Reference Information,” on page 111

Feedback

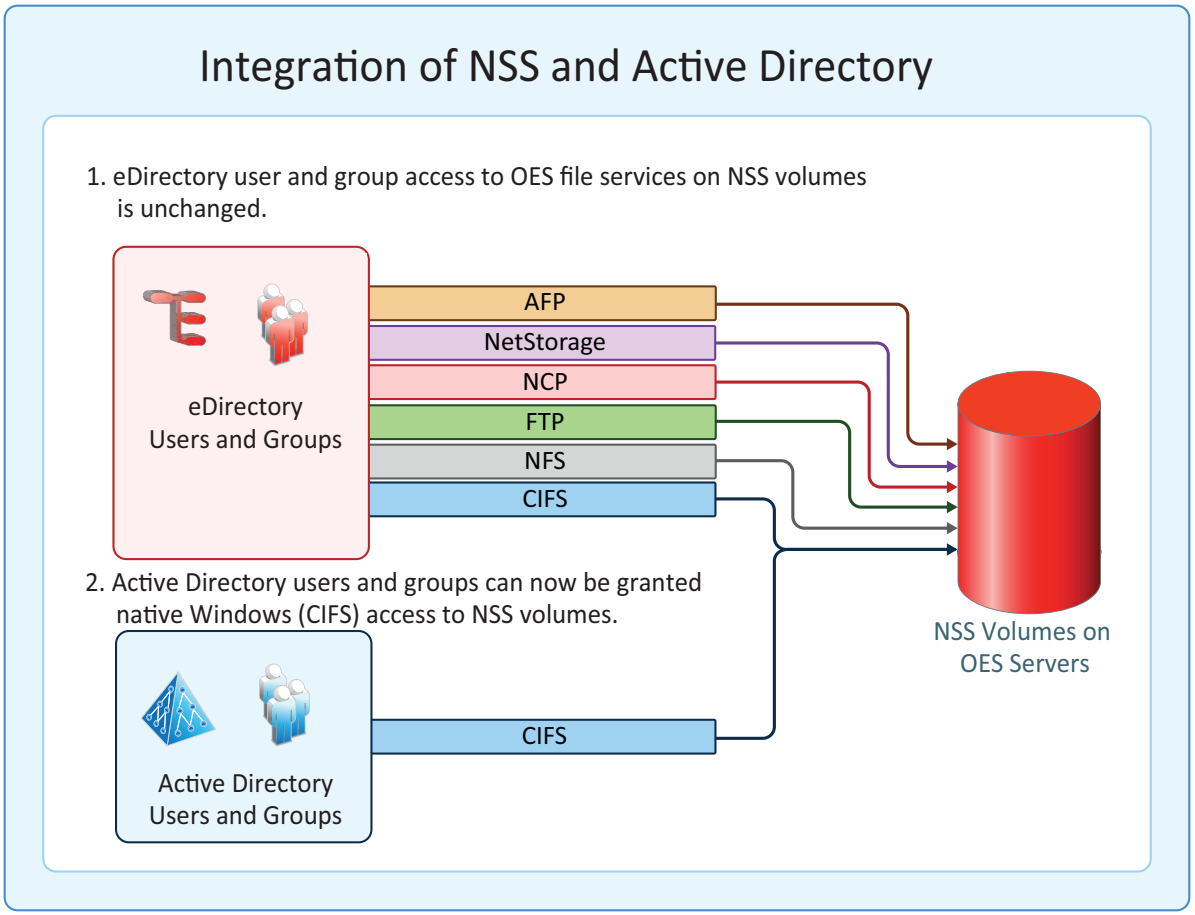
We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

For information about other OES products, see the OES 2023 Documentation Web Site.

1 Overview of NSS AD Support

Beginning with OES 2015 or later, you can provide Active Directory (AD) users with the ability to seamlessly access NSS resources and administer them. AD users and groups do not need to move to eDirectory; NSS resources can be accessed by both AD and eDirectory users at the same time.


Integration of NSS and Active Directory
1. eDirectory user and group access to OES file services on NSS volumes is unchanged.
eDirectory Users and Groups
AFP
NetStorage
NCP
FTP
NFS
CIFS
2. Active Directory users and groups can now be granted native Windows (CIFS) access to NSS volumes.
Active Directory Users and Groups
CIFS
NSS Volumes on OES Servers

1.1 Understanding What Changed to Enable NSS AD Support in OES

- Section 1.1.1, “OES CIFS Access Changes,” on page 10
- Section 1.1.2, “OES Service Changes For NSS AD,” on page 11
- Section 1.1.3, “Multi-Forest Support for AD Users,” on page 11
- Section 1.1.4, “Utility and Management Tool Changes,” on page 12

1.1.1 OES CIFS Access Changes

Figure 1-1 *OES CIFS Access Changes in OES*

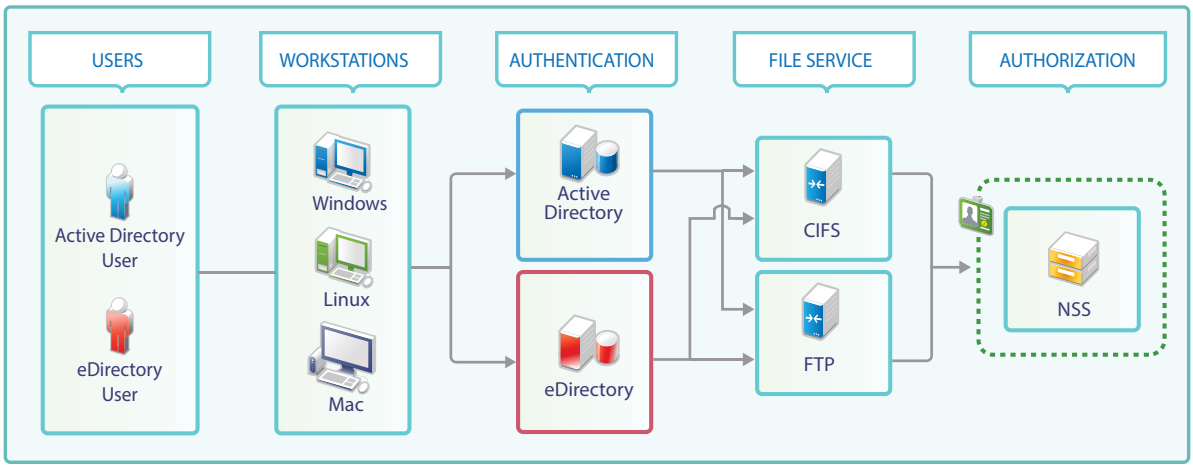


Table 1-1 *Summary of CIFS Access Changes*

CIFS Access Component	OES 11 SP2 and Earlier	OES 2015 and Later
Users	eDirectory users access NSS using their eDirectory credentials.	eDirectory and Active Directory users can access NSS using their eDirectory and Active Directory credentials, respectively.
Workstations	Windows, Linux and Macintosh are supported.	No changes in platform support.
Authentication	Only eDirectory is supported as an identity source. All file service access is controlled by eDirectory authentication through NMAS.	Both eDirectory and Active Directory are supported as identity sources. For eDirectory users, NMAS authentication is still used. For Active Directory users, CIFS interacts with Active Directory and the Kerberos service is used to authenticate the Active Directory users.
File Service	CIFS is among the many file services offered, which also include AFP, NetStorage, NCP, and FTP.	CIFS offers support for Active Directory users. Beginning with OES 2015 SP1, FTP offers support for Active directory users. No other file services are enabled for AD user access at this point.
Authorization	Authorization to access NSS is handled by CIFS working in cooperation with NSS.	Authorization to access NSS through CIFS is handled by NSS alone. This increases both the efficiency and the reliability of the authorization process.

1.1.2 OES Service Changes For NSS AD

Table 1-2 *OES Service Changes*

Service	OES Changes and Information
OES CIFS	You can grant AD users native CIFS access to NSS volumes with OES trustee model. ◆ Active Directory and eDirectory users can perform salvage and purge operation on Windows through NFARM (OES File Access Rights Management) utility. ◆ AD users can access NSS resources in a multi-forest environment. ◆ Beginning with OES 2018, Active Directory and eDirectory users can perform salvage and purge operation on Mac using NFARM (OES File Access Rights Management).
OES Cluster Services (NCS)	Cluster resources can now join to AD domains.
Distributed File Services (DFS)	DFS is supported in NSS AD environment.
Dynamic Storage Technology (DST)	DST is supported in NSS AD environment.
FTP Server	FTP server is supported in NSS AD environment.
Novell Identity Translator (NIT)	NIT lets you ensure that eDirectory and AD users requiring NSS authorization have the required UIDs. It supports AD users in multi-forest environment.
NSS (Storage Services)	AD users can now access NSS through CIFS.
Storage Management Services (SMS)	SMS now supports backing up AD trustee information in NSS AD environment.
NSS Auditing Client Logger (VLOG)	Audit all file operations for AD users. VLOG is enhanced to filter based on user names and application names.

1.1.3 Multi-Forest Support for AD Users

Beginning with OES 2015 SP1, multi-forest support allows access to NSS resources from Active Directory users belonging to AD forests having bi-directional trust with OES joined forest or AD domains having bi-directional external trust with OES joined forest.

The following OES components supports multi-forest for AD users: NSS, CIFS, DFS, DST, Migration Tool, NIT, SMS, and VLOG.

1.1.4 Utility and Management Tool Changes

Table 1-3 *OES Utility Changes*

Utility	Changes and Information
NFARM	Beginning with OES 2018, Active Directory and eDirectory users can perform salvage and purge operation on Mac. For more information, see NFARM Installer for Mac in the OES 2023: NSS File System Administration Guide for Linux.
nsscon	Options are added to update the SEV interval for AD users. Also, provided options to force update the SEV interval for AD users and for a single AD user. For more information, see Security Equivalence Vector Update Commands in the OES 2023: NSS File System Administration Guide for Linux.

2 What's New or Changed in NSS AD

This section describes enhancements and changes in NSS AD since the initial release Open Enterprise Server (OES) 2023.

- Section 2.1, "What's New or Changed in NSS AD (OES 2023)," on page 13

2.1 What's New or Changed in NSS AD (OES 2023)

In addition to the bug fixes, NSS AD provides the following enhancements and changes in OES 2023.

2.1.1 OES User Rights Map (NURM) Utility

Beginning with OES 2023, the OES User Rights Map (NURM) utility uses the latest version of Log4j and is installed with Log4j 2.x.

3 Preparing to Deploy NSS AD

Use the information in the following sections as you plan your NSS AD deployment.

- Section 3.1, “Software and Hardware Requirements,” on page 15
- Section 3.2, “Meeting NSS AD Infrastructure Requirements,” on page 15
- Section 3.3, “Joining OES to AD Domain When OES and AD are Present in Different DNS Domain,” on page 17
- Section 3.4, “Planning to Assign AD User and Group Trustee Rights,” on page 17
- Section 3.5, “Coexistence with NSS AD,” on page 18
- Section 3.6, “Caveats for Deploying NSS AD,” on page 20
- Section 3.7, “Joining OES to a DSfW Domain,” on page 21

3.1 Software and Hardware Requirements

NSS AD has no additional requirements beyond those outlined in “Meeting All Server Software and Hardware Requirements” in the *OES 2023: Installation Guide*.

3.2 Meeting NSS AD Infrastructure Requirements

You can select NSS AD pattern during OES installation or after the OES server is installed and running.

Table 3-1 *Preparing Your Infrastructure for OES*

	Selecting NSS AD pattern with OES Server installation	**Installing NSS AD post OES Server installation**
OES Server	Ensure to select the NSS AD pattern during OES server installation.	Ensure the OES server that will run NSS AD is fully patched (including SLES patches) before you install NSS AD.

	Selecting NSS AD pattern with OES Server installation	Installing NSS AD post OES Server installation
Active Directory	Ensure that your Active Directory deployment meets the following constraints: ◆ The Domain Controller for the domain your OES server will join is a Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, Windows 2016, or Windows 2019 server. ◆ Your NSS AD deployment targets can be a Single AD forest or Multi-forest environment. ◆ **Single Forest Environment:** Create a Universal Group with the sAMAccountName "OESAccessGrp" anywhere in the AD forest. Only the members of this group will have access to the NSS resources based on their trustee assignments. In absence of this group, all the AD users in the forest can access the NSS resources based on their trustee assignments. ◆ **Multi-Forest Environment:** Create a Domain Local Group (DLG) with the sAMAccountName "DLOESAccessGrp" in the AD domain to which this OES server is joined. Only the members of this group (OES forest and across forest) will have access to the NSS resources based on their trustee assignments. In absence of this group, the AD users across the forest cannot access the NSS resources.	
AD Rights	Identify the username and password of an AD user who has rights to join the OES server to the domain. The following rights are required on the container where the OES server object will be located: ◆ Reset password ◆ Create computer objects ◆ Delete computer objects ◆ Read and write the `msDs-supportedEncryptionTypes` attribute	
DNS	1. Ensure that the DNS service that the OES server will use is configured such that the server will be able to resolve the DNS name of the AD domain controller for the domain to which the server will be joined. 2. Ensure that the DNS service includes a reverse lookup entry for the AD domain controller.	1. Ensure that the OES server can resolve the DNS name of the AD domain controller for the domain that the server will join. 2. Ensure that the DNS service includes a reverse lookup entry for the AD domain controller.
CIFS	Install and configure CIFS at the same time as you install OES and NSS AD Support.	Ensure that the CIFS service that AD users will access is configured and operational on the OES server.
Time Synchronization	Ensure that the date and time settings that you specify for the OES server match those of the AD domain controller.	Ensure that the date and time for the OES server match the AD domain controller's date and time.

3.3 Joining OES to AD Domain When OES and AD are Present in Different DNS Domain

Consider the scenario where OES server is present in one DNS domain and AD server is present in another DNS domain. Before joining OES to AD domain, do the following:

- Ensure to meet the NSS AD requirements. For more information, see Prerequisites for Installing and Configuring NSS AD in the OES 2023: Installation Guide.
- The OES server should be able to resolve the DNS queries for the AD domain.

The example provides how to successfully join OES server to AD domain when OES and AD servers are in two different domains:

1. OES server is in *oesdomain.com* with the DNS server IP address *192.168.1.2*
2. AD server is joined to *addomain.com* with the DNS server IP address *192.168.20.22*
3. The DNS server with the IP address 192.168.1.2 should resolve the DNS queries on *addomain.com*. There are different ways to resolve the DNS queries, we have considered using DNS forwarder in this example:
   a. Configure the forwarder on 192.168.1.2 that points to 192.168.20.22
   b. Ensure all the PTR records exists for all Domain Controller (DC) and Global Catalog (GC) in 192.168.20.22
   c. From the OES server console, verify if the AD DC server and AD domain is resolvable.

      ```
      nslookup adserver1.addomain.com
      ```

      ```
      nslookup addomain.com
      ```

      The command should execute successfully and display details of the AD server and domain.

NOTE: For FTP AD remote navigation, ensure that the search attribute present in `/etc/resolv.conf` is configured with all the AD domain entries of the OES servers.

3.4 Planning to Assign AD User and Group Trustee Rights

Do the following:

1 Identify the Active Directory users and groups that need access to NSS resources.

2 You can assign the NSS trustee rights to your AD users and groups in two ways:

- Using NFARM (Windows explorer shell extension) or `rights` utility on the OES server. For more information about NFARM, see Section 7.5, “NFARM (OES File Access Rights Management),” on page 83 and rights in OES 2023: NSS File System Administration Guide for Linux.
- Using the NURM utility. This method assumes that at least some of your network users and groups have identities in both eDirectory and Active Directory that can be mapped to each other. For more information about NURM, see Section 7.4, “NURM (OES User Rights Map),” on page 71.

NOTE: If an AD user group membership is modified between the user login to AD domain and mapping to OES CIFS server, the AD user must logout and login again to the AD domain to perform the file operations on OES server.

3.5 Coexistence with NSS AD

The following sections cover NSS AD coexistence.

- Section 3.5.1, “Incompatiblities at a Server Level,” on page 18
- Section 3.5.2, “NSS AD Is Network-Compatible with All OES Services,” on page 18
- Section 3.5.3, “NSS AD Doesn’t Affect Backward Compatibility,” on page 18
- Section 3.5.4, “Ensuring DST Support for NSS AD,” on page 19
- Section 3.5.5, “DFS Deployment with NSS AD,” on page 19

3.5.1 Incompatiblities at a Server Level

Do not install the following service on the same server as NSS AD:

- **DSfW**

3.5.2 NSS AD Is Network-Compatible with All OES Services

Introducing NSS AD into your OES service mix will not cause any conflicts with existing OES services on your network.

3.5.3 NSS AD Doesn’t Affect Backward Compatibility

The following services and components, which were modified to support NSS AD, are compatible with pre-OES 2015 servers, with important exceptions noted.

- **Access Control Lists**
- **Backup (SMS)**
- **CIFS**
- **Distributed File Services (DFS)**
- **Dynamic Storage Technology (DST)**
- **OES Cluster Services (NCS)**

IMPORTANT: Pre-OES 2015 nodes cannot mount NSS-AD enabled pools and volumes. For more information, see Section 3.6.1, “Clustered Node Issue,” on page 20.

- **NSS (OES Storage Services)**
- **Salvage**

3.5.4 Ensuring DST Support for NSS AD

To provide NSS AD support in an environment that contains Dynamic Storage Technology (DST), you must do the following:

- Ensure that the OES server or the cluster node where the primary and shadow volumes exist, has joined the Active Directory domain as part of the normal NSS AD deployment process.
- Ensure that both the primary and the secondary (shadow) volumes are AD-enabled.

  The primary and secondary volumes can be of the same type (NSS32 or NSS64) or mixed (NSS32 and NSS64).
- The Linux utilities POSIX setxattr and POSIX setattr are enhanced to support DST. Any operation performed on a directory in the Primary volume is replicated on the shadow volumes for these utilities.

For more information on DST, see OES 2023: Dynamic Storage Technology Administration Guide.

3.5.5 DFS Deployment with NSS AD

- "DFS Source and Target Is NSS AD Enabled" on page 19
- "DFS in Heterogeneous Environment" on page 19

DFS Source and Target Is NSS AD Enabled

The DFS source and target server are configured with OES 2015 or later with NSS AD support. For AD users to access a DFS junction using the CIFS client, the following is required:

- The DFS source and the target server must have joined the AD domain.
- The pools and volumes present in DFS source and target server should be media-upgraded and AD-enabled respectively.
- AD users must have trustee rights on the files and folders they need to access.

DFS in Heterogeneous Environment

During the NSS AD deployment process, there is, of course, a period of time during which some servers are running NSS AD and some are not.

If the DFS source is NSS AD configured and the target is a pre-OES 2015 server, then for seamless access of data on the pre-OES 2015 server, ensure that both the Active Directory and eDirectory credentials have same usernames and passwords.

When the AD user accesses the pre-OES 2015 server, the CIFS client authenticates with the AD credentials and fails. CIFS then falls back to use eDirectory credentials and the user is able to access the data.

3.6 Caveats for Deploying NSS AD

Be aware of the following caveats before installing and configuring NSS AD.

- Section 3.6.1, “Clustered Node Issue,” on page 20
- Section 3.6.2, “Recommendations During Upgrade,” on page 20

3.6.1 Clustered Node Issue

Pre-OES 2015 servers cannot mount NSS-AD media-upgraded pools.

1. If possible, you should upgrade all cluster nodes to OES 2015 or later as part of your NSS-AD deployment.
2. If you cannot upgrade your cluster nodes at the same time, ensure the following:

   A mixed node cluster environment can contain OES 11 SP2, OES 2015, OES 2015 SP1, OES 2018, OES 2018 SP1, and OES 2018 SP2 nodes. The AD media upgraded NSS32 and NSS64 pools cannot be loaded in OES 11 SP2 nodes.

   When a resource comes online, it tries to load on a node based on the preferred node assignment (OES 2015 or later nodes), and the older OES cluster nodes are skipped from the preferred node list. If OES 2015 or later nodes are not available in the cluster, the resources are moved to “unassigned” state.

   However, if the upgraded (OES 2015 or later) node comes up or any new OES (OES 2015 or later) node is added to the cluster, the resource will automatically loads on the OES 2015 or later node.

IMPORTANT: ◆All nodes in the cluster must be patched with the latest OES patches. Otherwise, the AD media resource goes to comatose state on nodes earlier than OES 2015.

- All nodes in the cluster must belong to OES 11 SP2 or later. If any OES node in the cluster is older than OES 11 SP2, this feature does not work.

For more information, see “Configuring Preferred Nodes and Node Failover Order for a Resource” in the *OES 2023: OES Cluster Services for Linux Administration Guide*.

3.6.2 Recommendations During Upgrade

When upgrading the OES server, if NSS AD pattern is selected, then any misconfiguration in joining the domain can result in upgrade failure. Hence, it is recommended not to install NSS AD Support as part of the upgrade process. Instead, you must do the following:

1. Complete the upgrade/migration processes as documented in “ Upgrading to OES 2023” in the *OES 2023: Installation Guide*
2. Ensure that all of the NSS AD Infrastructure Requirements are met.
3. Run the YaST OES Installation module (or the NSS AD Support module) on the OES server and complete the applicable instructions in Chapter 4, “Installing and Configuring NSS AD Support,” on page 23.

For information on planning a migration to OES 2018 SP2, see the *OES 2023: Migration Tool Administration Guide*.

3.7 Joining OES to a DSfW Domain

OES server with NSS AD configured can join to any DSfW (Domain Services for Windows) domain, which allows DSfW users to access AD enabled NSS volumes over SMB protocol. DSfW users are considered same as AD users which enables them to perform authentication over kerberos. Management tools such as NURM and NFARM can be used by a DSfW user to manage the trustees, rights, quotas, salvage and purge. DSfW users can also access files from DST enabled and DFS enabled NSS volumes. Users of Active Directory domain which has bi-directional trust to DSfW domain can access the NSS volume.

Overall, OES server with NSS AD configured can join to AD or DSfW domain and users of cross forest AD or DSfW domain can seamlessly access the NSS volumes over SMB.

- Section 3.7.1, “Accessing NSS Over CIFS by eDirectory User Set As DSfW Users,” on page 21
- Section 3.7.2, “Accessing NSS Over CIFS by eDirectory Users As DSfW Users and DSfW Domain Having a Trust With One or More AD Domains/Forests,” on page 22

3.7.1 Accessing NSS Over CIFS by eDirectory User Set As DSfW Users

Name-mapped or non-name-mapped DSFW environment + eDirectory tree: OES is installed in the same eDirectory tree. The users from the eDirectory partition of DSFW domain access NSS over CIFS by using eDirectory credentials.

With NSS-AD support for DSfW, customers would like their users to access NSS over CIFS as DSFW domain users, thereby taking advantage of Single Sign-On through Kerberos.

As filesystem rights are already assigned to eDirectory users that there is no need to change the filesystem rights as the user set is same for both eDirectory and DSFW.

Planning the Environment

- All the servers joined to the DSFW domain should be OES 2018 SP2 or later.
- The user should access NSS by using either eDirectory or DSfW credentials. The same user should not access NSS by using both eDirectory and DSFW credentials.
- The eDirectory users accessing NSS will all be changed to access NSS as DSFW users over Kerberos.

Joining OES to the DSFW Domain

- Ensure to meet the NSS AD requirements. For more information, see Chapter 3, “Preparing to Deploy NSS AD,” on page 15.
- The OES server should resolve the DNS queries for the DSFW domain.
- Join OES server to the DSFW domain.

Enabling eDirectory Users to Access NSS Over CIFS As DSFW Users

1 By using `novcifs` command set `--map-adsessions-to-edir=YES` on the OES server.

By setting this option,

- The DSFW/AD domain users can access NSS over CIFS by using DSFW or AD credentials seamlessly.
- The filesystem operations are executed with the rights granted to their eDirectory identities.

2 On successful authentication the OES filesystem treats the connections as eDirectory connections.

Monitoring Connection

All the details related to connections in novcifs and NRM is listed as eDirectory connections.

3.7.2 Accessing NSS Over CIFS by eDirectory Users As DSfW Users and DSfW Domain Having a Trust With One or More AD Domains/ Forests

Name-mapped or non-name-mapped DSFW environment + DSfW Domain Trust with AD Forests/ Domains + eDirectory tree: AD and eDirectory have different user sets.

The DSFW and AD users authenticate by using their respective DSFW and AD credentials. However, file permissions for AD users shall be granted for their AD identities.

Planning the Environment

- Ensure to meet all the prerequisites listed in “Planning the Environment” on page 21.
- Users in the DSFW and AD environments should be unique.
- Join OES to DSFW domain.
- Enable file access for both DSFW and AD users.
- For AD users file permissions should be grated for their respective AD identities.
- Use `novcifs` command and set `--map-adsessions-to-edir=fallback` on the OES server.
- With this setting, file permissions on NSS for DSFW users are enforced using their eDirectory identities.

Monitoring Connections:

- All the connections from the DSfW users are listed as eDirectory connections.
- All the connections from the AD users are listed as AD connections.

4 Installing and Configuring NSS AD Support

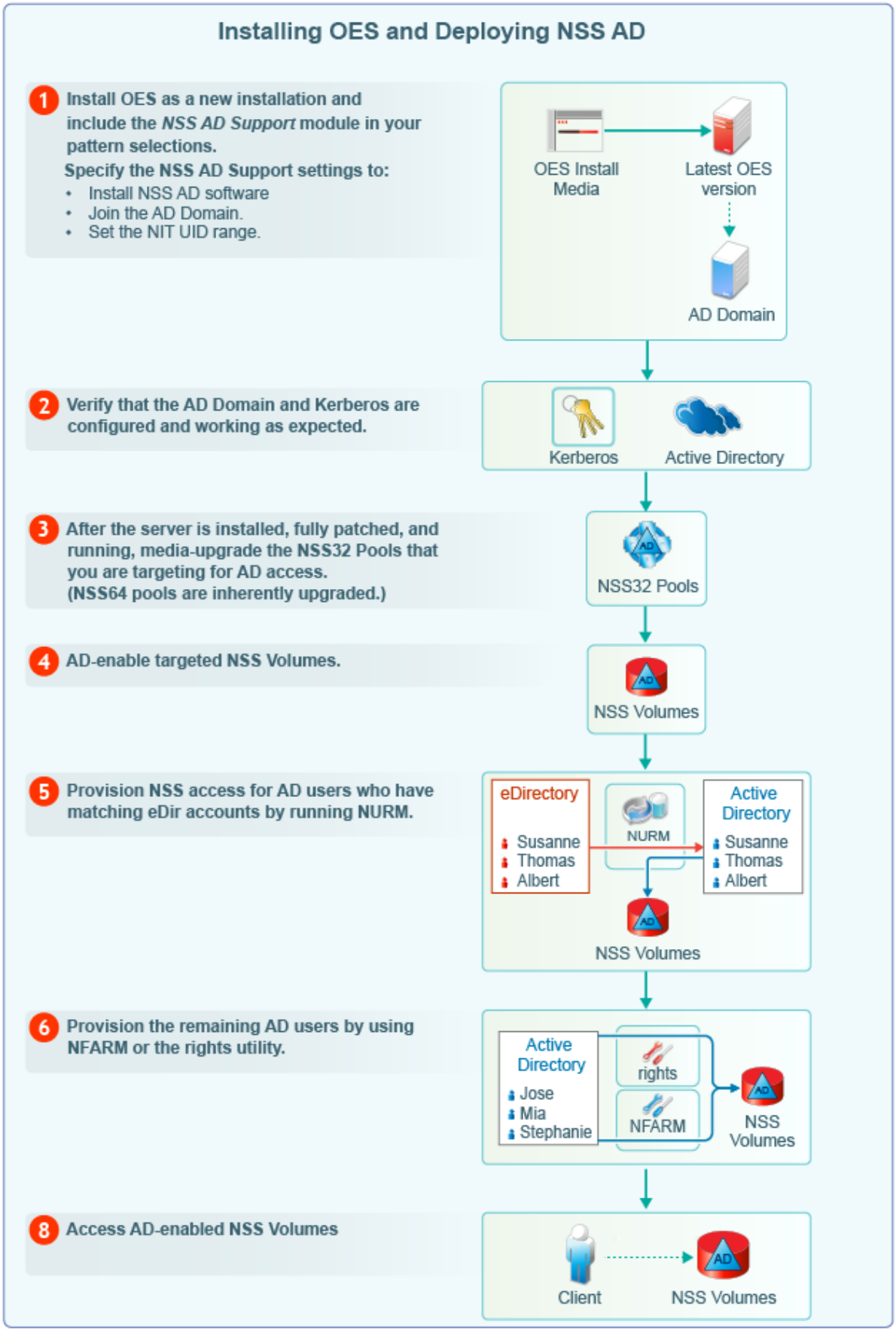
IMPORTANT: The information in this section supplements but does not replace the official OES installation and upgrade instructions that are contained in the OES 2023: Installation Guide.

This section covers the following topics:

- Section 4.1, “Installing a New OES Server and Deploying NSS AD,” on page 24
- Section 4.2, “Upgrading to OES 2018 SP2 and Deploying NSS AD (Non-Clustered Environment),” on page 32
- Section 4.3, “Upgrading to OES 2018 SP2 and Deploying NSS AD (Clustered Environment),” on page 39
- Section 4.4, “Leave a AD Domain,” on page 45
- Section 4.5, “Reconfiguring NSS AD,” on page 46
- Section 4.6, “Renaming the Netbios Name of OES Host or Cluster Resource,” on page 47

4.1 Installing a New OES Server and Deploying NSS AD

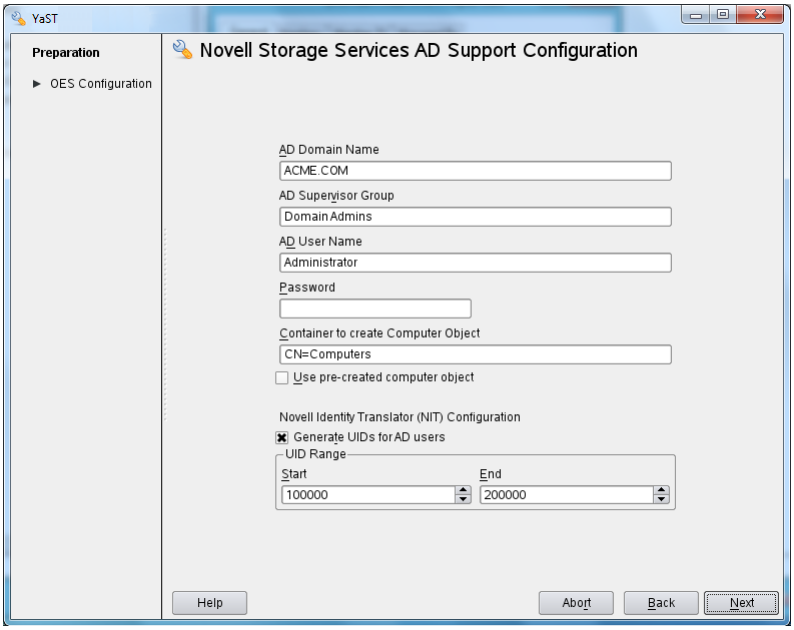
Figure 4-1 *Installing OES as a New Server and Deploying NSS AD*


Installing OES and Deploying NSS AD
1 Install OES as a new installation and include the NSS AD Support module in your pattern selections.
Specify the NSS AD Support settings to:
• Install NSS AD software
• Join the AD Domain.
• Set the NIT UID range.
OES Install Media
Latest OES version
AD Domain
2 Verify that the AD Domain and Kerberos are configured and working as expected.
Kerberos
Active Directory
3 After the server is installed, fully patched, and running, media-upgrade the NSS32 Pools that you are targeting for AD access. (NSS64 pools are inherently upgraded.)
NSS32 Pools
4 AD-enable targeted NSS Volumes.
NSS Volumes
5 Provision NSS access for AD users who have matching eDir accounts by running NURM.
eDirectory
Susanne
Thomas
Albert
NURM
Active Directory
Susanne
Thomas
Albert
NSS Volumes
6 Provision the remaining AD users by using NFARM or the rights utility.
Active Directory
Jose
Mia
Stephanie
rights
NFARM
NSS Volumes
8 Access AD-enabled NSS Volumes
Client
NSS Volumes

IMPORTANT: Before proceeding, ensure that you have met all the prerequisites specified in Section 3.2, “Meeting NSS AD Infrastructure Requirements,” on page 15.

If you want to install NSS AD after your OES server is installed and running, follow the instructions in Section 4.2, “Upgrading to OES 2018 SP2 and Deploying NSS AD (Non-Clustered Environment),” on page 32, starting with Step 2.

Table 4-1 *Installing OES and Deploying NSS AD*

Process	Information and Links
1	1. Using the instructions in the installation guide, install only one OES server at a time in your eDirectory tree. For detailed instructions, see "Installing OES 2023 as a New Installation" in the *OES 2023: Installation Guide*. 2. When you reach the **Software Selections** screen, select the **OES Storage Service AD Support** pattern along with the other services that you are installing.  3. Specify the required details: • **AD Domain Name:** Is the domain that the OES server is joining. • **AD Supervisor Group:** Is the AD supervisor group name. The AD users belonging to this group will have supervisory rights for all the volumes associated with that OES server. • **AD User Name:** Specify an AD administrator or user with the following privileges required to join the domain: ◦ Reset password ◦ Create computer objects ◦ Delete computer objects ◦ Read and write the `msDs-supportedEncryptionTypes` attribute. • **Password:** Is the password of the AD user who is used for the domain join operation. • **Container to Create Computer Object:** The container where the OES 2018 computer object will live. If you have already created a computer object in Active Directory for the OES server, select **Use pre-created computer object** and include the object name in the specification. • **Novell Identity Translator (NIT) Configuration:** NIT manages UIDs as required for data access on a Linux server. For more information, see "Section 7.2, "NIT (Novell Identity Translator)," on page 58". 4. When you click **Next**, you should receive a message that `The domain join is in progress`.

Process	Information and Links

2	1. Ensure that the OES computer object is created in the AD domain you specified.
	2. Verify that the default keytab entries for the OES server are created by entering the following command at the server's terminal prompt:
	`klist -k`
	For example:
	`tstsrv:~/Desktop #klist -k`
	`Keytab name: FILE:/etc/krb5.keytab`
	`KVNO Principal`
	`---- ---------------------------------`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`tstsrv:~/Desktop #`
	The 12 keytab entries represents the Service Principals of the OES server.
	3. You can also execute `kinit -k <name of the OES server>$` to ensure that the OES server is joined to the AD domain successfully.
	For example, `kinit -k tstsrv$`
	On successful execution of the above command, it does not display any output message and returns to terminal.

3	1. Media-upgrade the NSS32 pools that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Pools** c. Select a pool. d. Type `g`, then type `Y(es)` > `O(kay)`. e. Select another pool and continue until all of the NSS32 pools that AD users need access to are media-upgraded For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" in the *OES 2023: NSS File System Administration Guide for Linux*.

Process	Information and Links
4	1. AD-enable the NSS volumes that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Volumes** c. Select a volume. d. Type G, then type `Y(es) > O(kay)`. e. Select another volume and continue until all of the volumes that AD users need access to are AD-enabled. For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" in the *OES 2023: NSS File System Administration Guide for Linux*. See also, "AD-enable the Volume" in the *OES 2023: NSS File System Administration Guide for Linux*.
5	1. Review the information in Chapter 5, "Assigning NSS Trustee Rights for AD Users and Groups," on page 49 to ensure that you understand the trustee-assignment processes and the associated caveats, then continue with Step 2. 2. Assess whether the OES User Rights Map utility (NURM) applies to your organization by considering the following questions: a. Do any of your AD users and groups have matching eDirectory accounts? If so, you can use the OES User Rights Map utility (NURM) to map the rights between eDirectory and Active Directory users and groups and then apply NSS trustee assignments based on the mapping. If not, skip to process 6. b. Do you use NetIQ Identify Manager 4.5 or later to coordinate identities and passwords between Active Directory and eDirectory, and do you have a user map that was created using IDM Designer? If so, NURM can leverage that map. If not, you can create a map using NURM. c. Do you want to consolidate your overlapping eDirectory and Active Directory accounts to only Active Directory? If so, you can have NURM delete the eDirectory trustee assignments. 3. If applicable, run NURM to assign NSS trustee rights to your AD users. For more information, see Section 7.4, "NURM (OES User Rights Map)," on page 71.
6	1. For AD users and groups who need NSS access and do not have matching eDirectory accounts, you can grant trustee assignments using either the NFARM Windows shell extension or the `rights` utility. 2. Use other NSS tools to manage file and directory ownership, usage quotas and the other things that you manage for eDirectory users and groups. For more information, see "OES File Access Rights Management (NFARM)", "rights", "nsschown", and "nssquota" in the *OES 2023: NSS File System Administration Guide for Linux*.

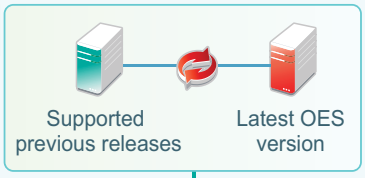
Process	Information and Links
7	To access the AD enabled NSS volumes, do the following: ◆ Ensure to create a forward lookup DNS entry for OES server where AD enabled NSS volumes are available. ◆ Map the NSS volume with the complete DNS name of the OES server or host name (not with the IP address).

4.2 Upgrading to OES 2018 SP2 and Deploying NSS AD (Non-Clustered Environment)

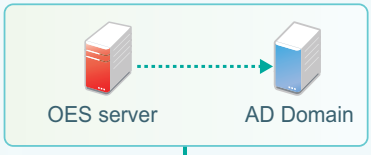
Figure 4-2 *Upgrading to OES 2018 SP2 and Deploying NSS AD in a Non-Clustered Environment*

Upgrading a Server and Deploying NSS AD (Non-Clustered Environment)

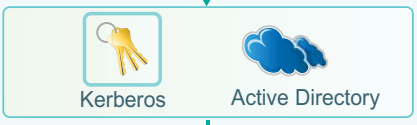
1. **Upgrade the OES server to latest OES version.**



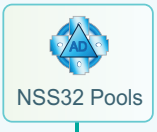
2. **On the fully upgraded and patched server, run YaST and install the NSS AD Support module to:**
   - Install NSS AD software
   - Join the AD Domain.
   - Set the NIT UID range.



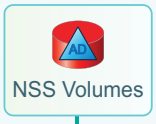
3. **Verify that the AD Domain and Kerberos are configured and working as expected.**



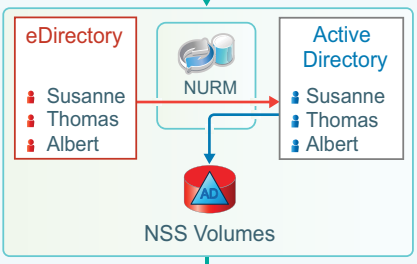
4. **NSS-AD Media-upgrade targeted NSS32 Pools. (NSS64 pools are inherently upgraded.)**



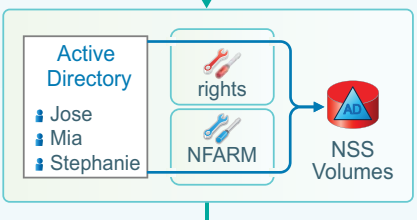
5. **AD-enable targeted NSS Volumes.**



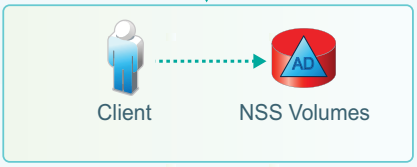
6. **Provision NSS access for AD users who have matching eDir accounts by running NURM.**



7. **Provision the remaining AD users by using NFARM or the rights utility.**



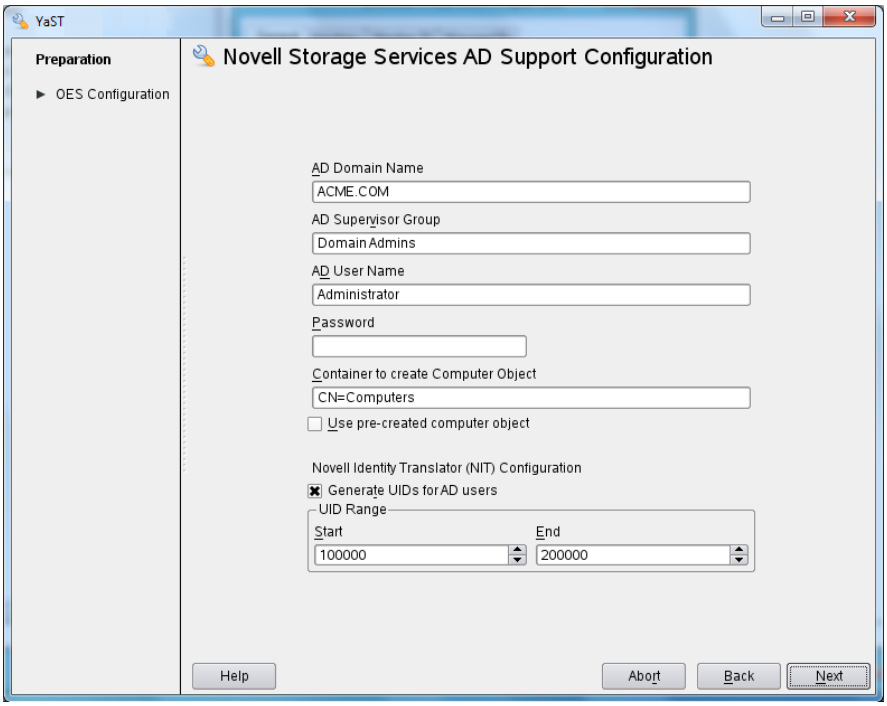
8. **Access AD-enabled NSS Volumes**



IMPORTANT: Before proceeding, ensure that you have met all the prerequisites specified in Section 3.2, “Meeting NSS AD Infrastructure Requirements,” on page 15.

Table 4-2 *Upgrading to OES 2018 SP2 and Deploying NSS AD*

Process	Information and Links
1	Using the instructions in the installation guide, upgrade only one server in your tree at a time. **IMPORTANT:** When upgrading the OES server, if NSS AD pattern is selected, then any misconfiguration in joining the domain can result in upgrade failure. Hence, it is recommended not to install NSS AD Support as part of the upgrade process. For detailed instructions, see “ Upgrading to OES 2023” in the *OES 2023: Installation Guide*.

Process	Information and Links
2	1. On the OES server, run YaST and when you reach the **Software Selections** screen, select the **OES Storage Service AD Support** pattern. 2. When you reach the **YaST OES Patterns** screen, select the **OES Storage Service AD Support** pattern.  3. Specify the required details: • **AD Domain Name:** Is the domain that the OES server is joining. • **AD Supervisor Group:** Is the AD supervisor group name. The AD users belonging to this group will have supervisory rights for all the volumes associated with that OES server. • **AD User Name:** Specify an AD administrator or user with the following privileges required to join the domain: ◦ Reset password ◦ Create computer objects ◦ Delete computer objects ◦ Read and write the `msDs-supportedEncryptionTypes` attribute. • **Password:** Is the password of the AD user who is used for the domain join operation. • **Container to Create Computer Object:** The container where the OES 2018 computer object will live. If you have already created a computer object in Active Directory for the OES server, select **Use pre-created computer object** and include the object name in the specification. • **Novell Identity Translator (NIT) Configuration:** NIT manages UIDs as required for data access on a Linux server. For more information, see "Section 7.2, "NIT (Novell Identity Translator)," on page 58". 4. When you click **Next**, you should receive a message that `The domain join is in progress`.

Process	Information and Links

3	1. Ensure that the OES computer object is created in the AD domain you specified.
	2. Verify that the default keytab entries for the OES server are created by entering the following command at the server's terminal prompt:
	`klist -k`
	For example:
	`tstsrv:~/Desktop #klist -k`
	`Keytab name: FILE:/etc/krb5.keytab`
	`KVNO Principal`
	`---- --------------------------------`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`tstsrv:~/Desktop #`
	The 12 keytab entries represents the Service Principals of the OES server.
	3. You can also execute `kinit -k <name of the OES server>$` to ensure that the OES server is joined to the AD domain successfully.
	For example, `kinit -k tstsrv$`
	On successful execution of the above command, it does not display any output message and returns to terminal.

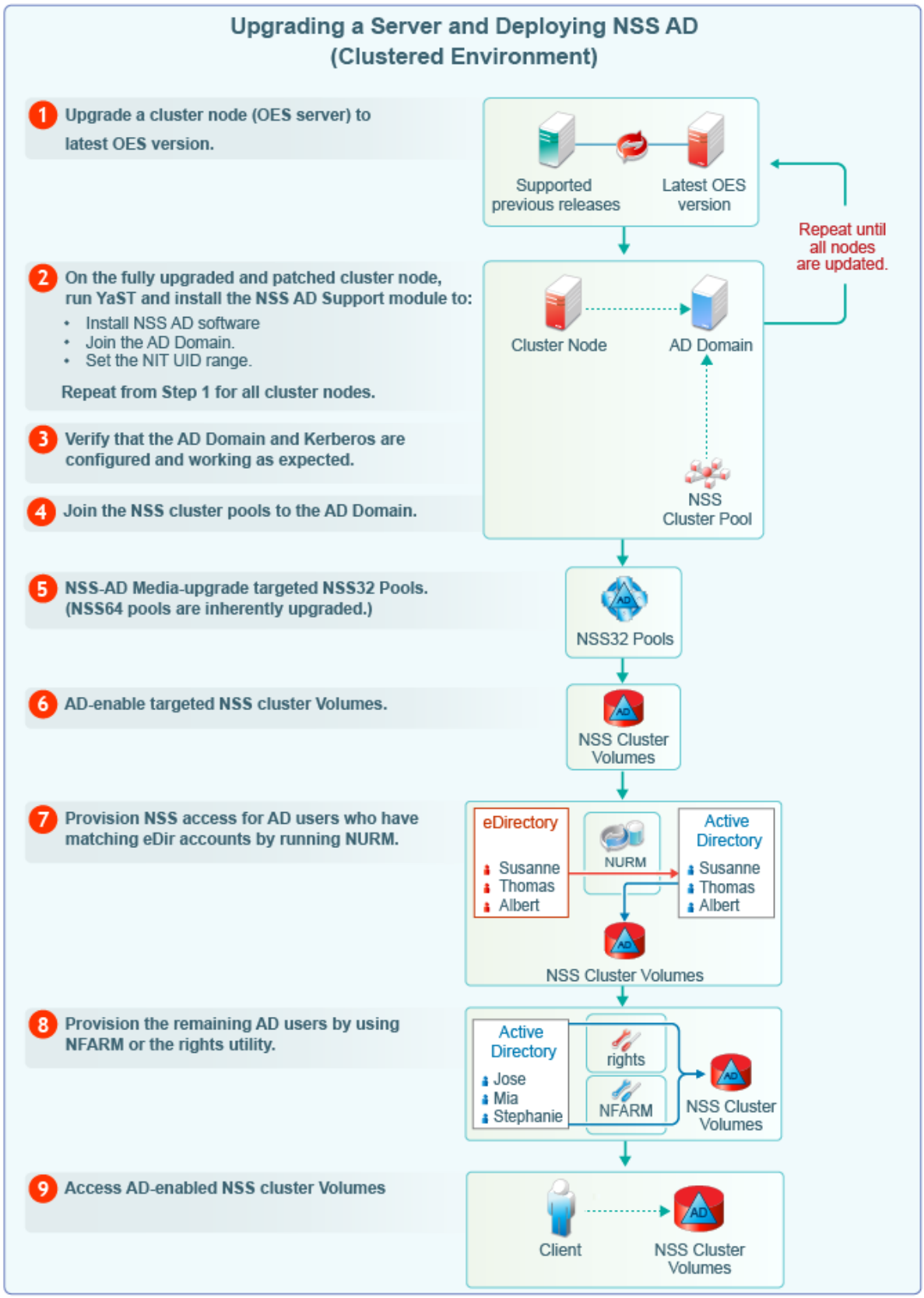
4	1. Media-upgrade the NSS32 pools that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Pools** c. Select a pool. d. Type `g`, then type `Y(es)` > `0(kay)`. e. Select another pool and continue until all of the NSS32 pools that AD users need access to are media-upgrated For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" in the *OES 2023: NSS File System Administration Guide for Linux*.

Process	Information and Links
5	1. AD-enable the NSS volumes that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Volumes** c. Select a volume. d. Type G, then type `Y(es) > O(kay)`. e. Select another volume and continue until all of the volumes that AD users need access to are AD-enabled. For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" in the *OES 2023: NSS File System Administration Guide for Linux*. See also, "AD-enable the Volume" in the *OES 2023: NSS File System Administration Guide for Linux*.
6	1. Review the information in Chapter 5, "Assigning NSS Trustee Rights for AD Users and Groups," on page 49 to ensure that you understand the trustee-assignment processes and the associated caveats, then continue with Step 2. 2. Assess whether the OES User Rights Map utility (NURM) applies to your organization by considering the following questions: a. Do any of your AD users and groups have matching eDirectory accounts? If so, you can use the OES User Rights Map utility (NURM) to map the rights between eDirectory and Active Directory users and groups and then apply NSS trustee assignments based on the mapping. If not, skip to process 7. b. Do you use NetIQ Identify Manager 4.5 or later to coordinate identities and passwords between Active Directory and eDirectory, and do you have a user map that was created using IDM Designer? If so, NURM can leverage that map. If not, you can create a map using NURM. c. Do you want to consolidate your overlapping eDirectory and Active Directory accounts to only Active Directory? If so, you can have NURM delete the eDirectory trustee assignments. 3. If applicable, run NURM to assign NSS trustee rights to your AD users. For more information, see Section 7.4, "NURM (OES User Rights Map)," on page 71.
7	1. For AD users and groups who need NSS access and do not have matching eDirectory accounts, you can grant trustee assignments using either the NFARM Windows shell extension or the `rights` utility. 2. Use other NSS tools to manage file and directory ownership, usage quotas and the other things that you manage for eDirectory users and groups. For more information, see "OES File Access Rights Management (NFARM)", "rights", "nsschown", and "nssquota" in the *OES 2023: NSS File System Administration Guide for Linux*.

Process	Information and Links
8	To access the AD enabled NSS volumes, do the following: ◆ Ensure to create a forward lookup DNS entry for OES server where AD enabled NSS volumes are available. ◆ Map the NSS volume with the complete DNS name of the OES server or host name (not with the IP address).

4.3 Upgrading to OES 2018 SP2 and Deploying NSS AD (Clustered Environment)

Figure 4-3 *Upgrading to OES 2018 SP2 and Deploying NSS AD in a Clustered Environment*

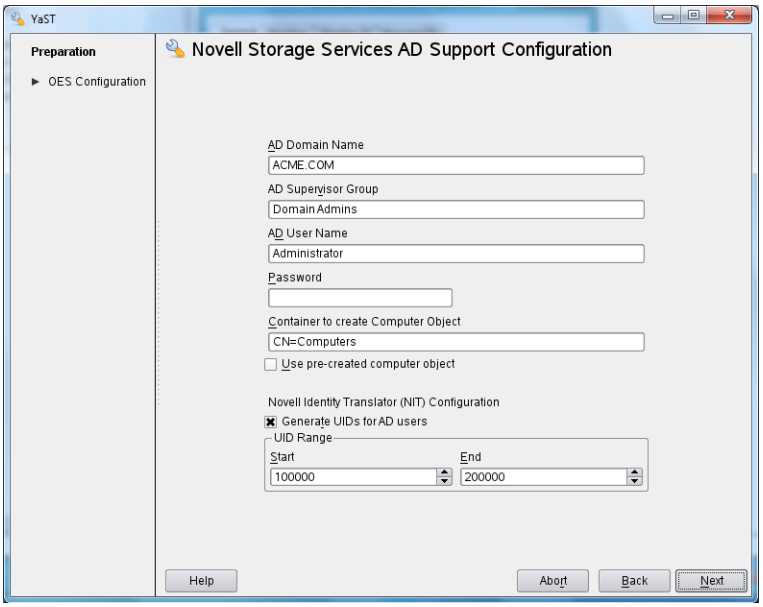

Upgrading a Server and Deploying NSS AD
(Clustered Environment)
1 Upgrade a cluster node (OES server) to latest OES version.
Supported previous releases
Latest OES version
Repeat until all nodes are updated.
2 On the fully upgraded and patched cluster node, run YaST and install the NSS AD Support module to:
• Install NSS AD software
• Join the AD Domain.
• Set the NIT UID range.
Repeat from Step 1 for all cluster nodes.
Cluster Node
AD Domain
3 Verify that the AD Domain and Kerberos are configured and working as expected.
4 Join the NSS cluster pools to the AD Domain.
NSS Cluster Pool
5 NSS-AD Media-upgrade targeted NSS32 Pools. (NSS64 pools are inherently upgraded.)
NSS32 Pools
6 AD-enable targeted NSS cluster Volumes.
NSS Cluster Volumes
7 Provision NSS access for AD users who have matching eDir accounts by running NURM.
eDirectory
Susanne
Thomas
Albert
NURM
Active Directory
Susanne
Thomas
Albert
NSS Cluster Volumes
8 Provision the remaining AD users by using NFARM or the rights utility.
Active Directory
Jose
Mia
Stephanie
rights
NFARM
NSS Cluster Volumes
9 Access AD-enabled NSS cluster Volumes
Client
NSS Cluster Volumes

IMPORTANT: Before proceeding, ensure that you have met all the prerequisites specified in Section 3.2, “Meeting NSS AD Infrastructure Requirements,” on page 15.

Table 4-3 *Upgrading to OES 2018 SP2 and Deploying NSS AD*

Process	Information and Links
1	1. Using the instructions in the installation guide, upgrade only one cluster node in your tree at a time. **IMPORTANT:** When upgrading the OES server, if NSS AD pattern is selected, then any misconfiguration in joining the domain can result in upgrade failure. Hence, it is recommended not to install NSS AD Support as part of the upgrade process. For more information about upgrading OES Clusters, see “Upgrading OES Clusters” in the *OES 2023: OES Cluster Services for Linux Administration Guide*.

Process	Information and Links
2	1. On the cluster node (OES server), run YaST and when you reach the **Software Selections** screen, select the **OES Storage Service AD Support** pattern.



2. Specify the following details:
   - **AD Domain Name:** The AD domain that the OES server is joining.
   - **AD Supervisor Group:** Is the AD supervisor group name. The AD users belonging to this group will have supervisory rights for all the volumes associated with that OES server.
   - **AD User Name:** Specify an AD administrator or user with the following privileges required to join the domain:
     - Reset password
     - Create computer objects
     - Delete computer objects
     - Read and write the `msDs-supportedEncryptionTypes` attribute.
   - **Password:** Is the password of the AD user who is used for the domain join operation.
   - **Container to Create Computer Object:** The container where the OES 2018 computer object either has been or will be created.

     If you have already created a computer object in Active Directory for the OES server, select **Use pre-created computer object**.
   - **Novell Identity Translator (NIT) Configuration:** NIT generates UIDs as required for anyone accessing data on a Linux server. For more information on NIT, see "Section 7.2, "NIT (Novell Identity Translator)," on page 58".

     If you want NIT to generate UIDs for AD users, select **Generate UID for AD users**, then specify the UID range. If you want NIT to retrieve UIDs from Active Directory, do not select the **Generate UID for AD users** option.

     For more information about this option, see "Table 7-2 on page 60."
3. When you click Next, the server/node is joined to the AD domain.

   For more information about joining cluster nodes to the AD domain, see "Joining the Cluster Node to an Active Directory Domain" in the *OES 2023: OES Cluster Services for Linux Administration Guide*.

Process	Information and Links

3	Verify the AD domain and Kerberos is configured and working in all the cluster nodes.
	1. Ensure that the OES computer object is created in the AD domain you specified.
	2. Verify that the default keytab entries for the OES server are created by entering the following command at the server's terminal prompt:
	`klist -k`
	For example:
	`tstsrv:~/Desktop #klist -k`
	`Keytab name: FILE:/etc/krb5.keytab`
	`KVNO Principal`
	`---- --------------------------------`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 tstsrv$@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv.acme.com@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 cifs/tstsrv@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`2 host/tstsrv.acme.com@ACME.COM`
	`tstsrv:~/Desktop #`
	The 12 keytab entries represents the Service Principals of the OES server.
	3. You can also execute `kinit -k <name of the OES server>$` to ensure that the OES server is joined to the AD domain successfully.
	For example, `kinit -k tstsrv$`
	On successful execution of the above command, it does not display any output message and returns to terminal.

4	1. Ensure that CIFS is chosen as the advertizing protocol for the cluster resource. NSS resource access for AD users happens only through the CIFS protocol. For more information, see "Adding Advertising Protocols for NSS Pool Cluster Resources" in the *OES 2023: OES Cluster Services for Linux Administration Guide*. 2. Join the cluster pool to the AD domain by following the instructions in "Joining Cluster Pools to the AD Domain" in the *OES 2023: NSS File System Administration Guide for Linux* or "Joining the Cluster Resource to an Active Directory Domain" in the *OES 2023: OES Cluster Services for Linux Administration Guide*. You can also use the following tools: ◆ The `novell-ad-util` CLI tool for joining the domain. See Section 7.3.1, "novell-ad-util Command Line Utility," on page 65. ◆ NSSMU. See "NSS Management Utility (NSSMU) Quick Reference" in the *OES 2023: NSS File System Administration Guide for Linux*. 3. Verify the Service Principal Names and computer objects by completing the steps in "Verifying the Service Principals and Computer Objects" in the *OES 2023: OES Cluster Services for Linux Administration Guide*.

Process	Information and Links
5	1. Media-upgrade your NSS32 cluster pools that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Pools** c. Select a pool. d. Type `g`, then type `Y(es) > 0(kay)`. e. Select another pool and continue until all of the NSS32 cluster pools that AD users need access to are media-upgraded For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" and "Upgrading the NSS Media Format" in the *OES 2023: NSS File System Administration Guide for Linux*.
6	1. AD-enable the NSS volumes that your AD users need access to. The following is a simple, GUI-driven method. a. At a terminal prompt, enter `nssmu`. b. Select **Volumes** c. Select a volume. d. Type `G`, then type `Y(es) > 0(kay)`. e. Select another volume and continue until all of the volumes that AD users need access to are AD-enabled. For more information on the NSS Media upgrade options and processes, see "NSS Media Upgrade Commands" in the *OES 2023: NSS File System Administration Guide for Linux*. See also, "AD-enable the Volume" and "Volume AD-enabling"in the *OES 2023: NSS File System Administration Guide for Linux*.

Process	Information and Links
7	1. Review the information in Chapter 5, "Assigning NSS Trustee Rights for AD Users and Groups," on page 49 to ensure that you understand the trustee-assignment processes and the associated caveats, then continue with Step 2. 2. Assess whether the OES User Rights Map utility (NURM) applies to your organization by considering the following questions: a. Do any of your AD users and groups have matching eDirectory accounts? If so, you can use the OES User Rights Map utility (NURM) to map the rights between eDirectory and Active Directory users and groups and then apply NSS trustee assignments based on the mapping. If not, skip to process 8. b. Do you use NetIQ Identify Manager 4.5 or later to coordinate identities and passwords between Active Directory and eDirectory, and do you have a user map that was created using IDM Designer? If so, NURM can leverage that map. If not, you can create a map using NURM. c. Do you want to consolidate your overlapping eDirectory and Active Directory accounts to only Active Directory? If so, you can have NURM delete the eDirectory trustee assignments. 3. If applicable, run NURM to assign NSS trustee rights to your AD users. For more information, see Section 7.4, "NURM (OES User Rights Map)," on page 71.
8	1. For AD users and groups who need NSS access and do not have matching eDirectory accounts, you can grant trustee assignments using either the NFARM Windows shell extension or the `rights` utility. 2. Use other NSS tools to manage file and directory ownership, usage quotas and the other things that you manage for eDirectory users and groups. For more information, see "OES File Access Rights Management (NFARM)", "rights", "nsschown", and "nssquota" in the *OES 2023: NSS File System Administration Guide for Linux*.
9	To access the AD enabled NSS cluster volumes, do the following: ◆ Ensure to create a forward lookup DNS entry for netbios name of the cluster resource. ◆ Map the NSS cluster volumes with the complete DNS name created for the cluster resource or with the short name of the netbios name of cluster resource (not with the IP address).

4.4 Leave a AD Domain

Use `novell-ad-util` to disjoin an OES server from the AD domain. Using YaST or NSSMU, you cannot disjoin from the AD domain.

To disjoin the OES host from the Active Directory domain, execute the following:

1. `kinit Administrator@EXAMPLE.COM`

Authenticates the administrator with the AD server, where "Administrator" is the domain admin or user with the sufficient rights and "EXAMPLE.COM" is the AD domain.

2. `novell-ad-util --leave-domain --domain-name EXAMPLE.COM`

To disjoin a cluster resource from the Active Directory domain, execute the following:

1. `kinit Administrator@EXAMPLE.COM`

   Authenticates the administrator with the AD server, where "Administrator" is the domain admin or user with the sufficient rights and "EXAMPLE.COM" is the AD domain.

2. Run the following command on the node where the cluster resource is running.

   ```
   novell-ad-util --leave-domain --cluster-resource .cn=CLUSTER-OES2018-
   POOLSERVER.o=novell.t=NSSAD_CLUSTER. --domain-name EXAMPLE.COM
   ```

3. Run the following command on all the cluster nodes except the node where step 2 is performed.

   ```
   novell-ad-util --purge 0 --cluster-resource .cn=CLUSTER-OES2018-
   POOLSERVER.o=novell.t=NSSAD_CLUSTER.
   ```

   Removes all the keytab entries of the cluster resource specified in the default keytab file.

Verifying the Domain Leave

To ensure that the domain leave is successful, verify the following:

1. Computer objects in the AD domain representing the OES host and cluster resources are removed.
2. Keytab entries are removed from `/etc/krb5.keytab`.
   - `klist -k | grep <netbios name of OES host>`

     It should be empty after the OES host leaves the domain.
   - `klist -k | grep <netbios name of a cluster resource>`

     Execute this command from all the cluster nodes. It should be empty after the cluster resource leaves the domain.

4.5 Reconfiguring NSS AD

If the OES host server or cluster resource is already joined to an AD domain and you need to join the same OES host server or the cluster resource to a different AD domain, then you need to reconfigure NSS AD using YaST.

Before reconfiguring NSS AD, ensure to leave the AD domain. For more information, see “Leave a AD Domain” on page 45.

After leaving the AD domain, perform the following to reconfigure NSS AD:

1. Ensure that the AD requirements are met before reconfiguring the NSS AD. For more information, see Section 3.2, “Meeting NSS AD Infrastructure Requirements,” on page 15.
2. Join to a AD domain. The AD domain can be the domain that was joined earlier or a different AD domain. For more information, see step 2, step 3 and step 4 of process 1 and process 2 in the Table 4-1 on page 27.

4.6 Renaming the Netbios Name of OES Host or Cluster Resource

To rename the netbios name of a OES host or a cluster resource, perform the following:

1. Leave the domain. For more information, see “Leave a AD Domain” on page 45.
2. Using iManager, rename the netbios name also known as CIFS Virtual Server Name. For more information, see Setting CIFS General Server Parameters in the OES 2023: OES CIFS for Linux Administration Guide.
3. Reconfigure NSS AD. For more information, see “Reconfiguring NSS AD” on page 46.

5 Assigning NSS Trustee Rights for AD Users and Groups

- Section 5.1, “Overview of the Provisioning Process,” on page 49
- Section 5.2, “NURM Provisioning Caveats,” on page 50

5.1 Overview of the Provisioning Process

Novell provides a number of tools to help you provision your AD users and groups for NSS access. Figure 5-1 provides a high-level overview of the provisioning process.

Figure 5-1 *Provisioning AD User and Groups for NSS Access*

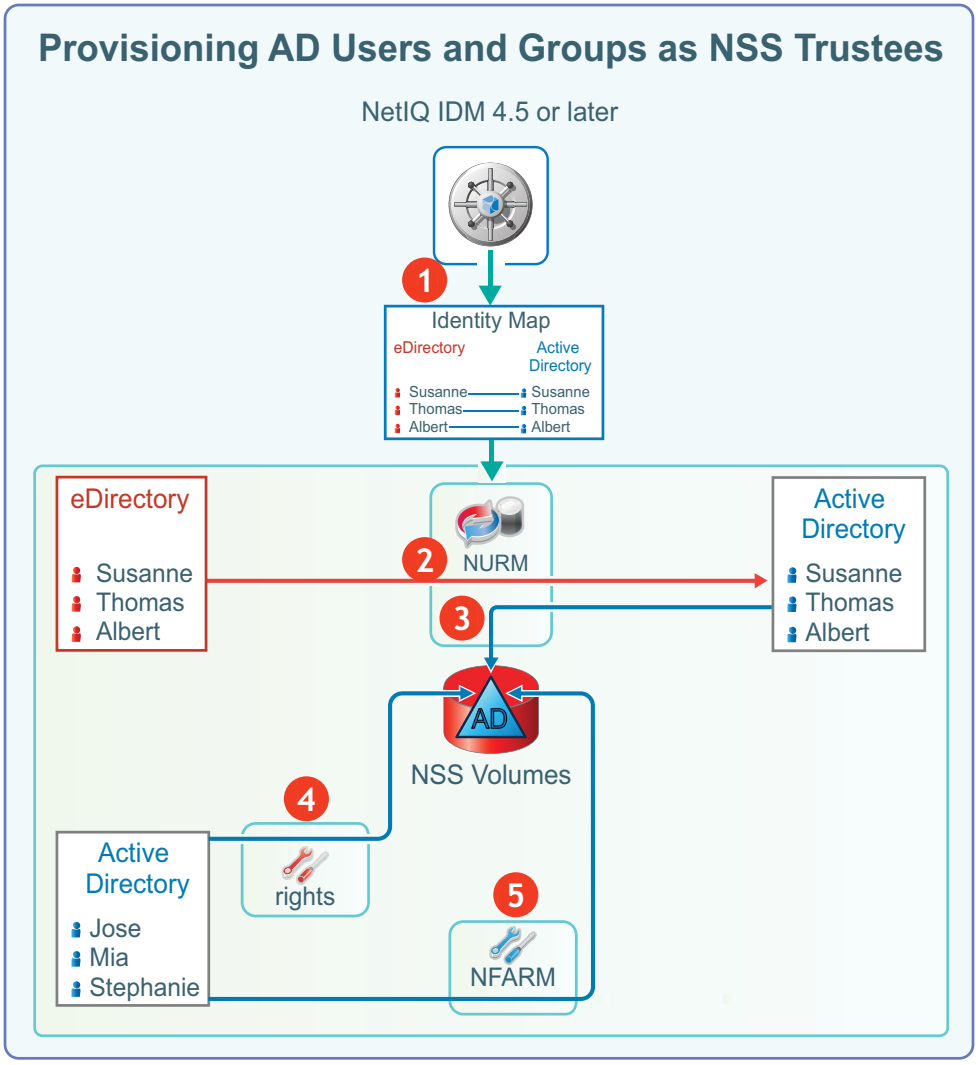


Table 5-1 Upgrading to OES 2018 SP2 and Deploying NSS AD

Step	Information and Links
1	◆ If you have NetIQ IDM 4.5 or later, and you have created an Active Directory to eDirectory user map using IDM Designer (not the IDM iManager plug-in), the User Resource Map utility (NURM) can leverage the map for replicating NSS ACLS for eDirectory users and groups to NSS ACLs for corresponding AD users and groups. Select the IDM option to use a map file in eDirectory. **IMPORTANT:** Ensure that the eDirectory user entered in NURM has access to the `DirXML-ADContext` attribute in eDirectory from the administrative workstation where you will run NURM.
2	◆ If you don't have an applicable Active Directory to eDirectory user map, NURM helps you create one.
3	◆ After you have verified the user map and the rights to be assigned to the users and groups, you can apply the rights to the selected NSS volume.
4	◆ To enable AD users and groups that don't have corresponding eDirectory accounts, you can use the `rights` CLI command at the server's terminal prompt.
5	◆ You can also use the NFARM Windows shell extension to assign NSS trustee rights to AD users and groups.

5.2 NURM Provisioning Caveats

- Section 5.2.1, "iManager Created NetIQ IDM Map Files Do Not Work with NURM," on page 50
- Section 5.2.2, "NURM eDirectory User Must Have a CIFS Universal Password Policy," on page 50

5.2.1 iManager Created NetIQ IDM Map Files Do Not Work with NURM

To use an IDM-created user map, NURM requires that the map be located in the `DirXML-ADContext` attribute in eDirectory.

IDM Designer stores the map in the `DirXML-ADContext` attribute; the IDM iManager plug-in does not.

For more information on creating the IDM drivers using IDM Designer, see Creating the Driver in Designer in the NetIQ Driver for Active Directory Implementation Guide.

5.2.2 NURM eDirectory User Must Have a CIFS Universal Password Policy

The eDirectory user that you specify in the NURM dialog must have the same universal password policy assigned as your eDirectory CIFS users.

IMPORTANT: This applies to the eDirectory Admin and any container admins you might choose to specify when running NURM.

6 Managing NSS AD

Table 6-1 outlines tools and tips for different the management areas associated with NSS AD Support.

Table 6-1 *Managing NSS AD Support*

Subject	Tools and Tips
AD Administrator Supervision of AD-enabled Volumes:	◆ Members of the `Domain Admins` group in the domain that a OES server joins, have supervisory rights for all the AD-enabled volumes associated with that server. ◆ To change the supervisor group for a server, enter the following command at the server's terminal prompt: `nitconfig set ad-supervisor-group=AD-group-name`
Consolidate Storage to NSS	◆ If your eDirectory users access NSS, your Active Directory users access NTFS, and you want to consolidate your storage on NSS, you can retain both identity sources and use NFARM to manage the trustee rights and quotas of AD users. ◆ You can also use the NSS `rights` and `quota` utilities to manage the rights and quotas of AD users and groups. ◆ You can continue to use both eDirectory and Active Directory as is, or you can consolidate all identities to Active Directory and continue to use the NSS file system.
Mass ACL Assignment	◆ OES User Rights Management (NURM)
Move and Split AD-enabled Volumes	◆ Distributed File Services iManager plug-in see "Guidelines for Moving or Splitting NSS Volumes" and "Active Directory Environment" in the *OES 2023: Distributed File Services Administration Guide for Linux*.

Subject	Tools and Tips
NSS	◆ iManager Media-upgrade an NSS32 pool at the time of pool creation. AD-enable a volume during or after volume creation. ◆ NRM Manage DST Policies, primary and secondary volumes, and so on. ◆ NSSMU Media-upgrade existing NSS32 pools. AD-enable existing volumes. ◆ NLVM Specify the pool type as NSS64 or NSS32 (default). Force the creation of a 64-bit pool in a cluster with pre-OES 2015 servers. Display all size outputs in a specified human-readable format.
Quotas	**For AD Users and Groups** ◆ OES File Access and Rights Management (NFARM) See Section 7.5.4, “Managing the Trustee Rights in the NSS File System,” on page 86 ◆ `quota` utility See “nssquota” in the *OES 2023: NSS File System Administration Guide for Linux* **For eDirectory Users and Groups** ◆ iManager ◆ `quota` utility See “nssquota” in the *OES 2023: NSS File System Administration Guide for Linux*
Restrict General AD User Access	To restrict NSS resource access for Active Directory users and groups: 1. Create a universal group anywhere in the AD forest 2. Specify its `sAMAccountName` as `OESAccessGrp` Only the members of this group will have NSS resource access based on their trustees assignments. If this group does not exist, all Active Directory users and groups in the forest can access the NSS resources based on their trustee assignments. Only one `OESAccessGrp` universal group can be created for an AD forest.

Subject	Tools and Tips
Allow AD User Access in Multi-Forest Environment	To allow NSS resource access for Active Directory users and groups in Multi-forest environment: 1. Create a Domain Local Group (DLG) in the AD domain to which OES server is joined. 2. Specify its `sAMAccountName` as `DLOESAccessGrp` Only the members of this group (OES forest and across forest) has access to NSS resources based on their trustees assignments. In absence of this group, the AD users across the forest cannot access the NSS resources.
Trustee Rights on AD-enabled NSS Volumes	**For AD Users and Groups** ◆ OES File Access and Rights Management (NFARM) ◆ `rights` utility **For eDirectory Users and Groups** ◆ iManager ◆ `rights` utility ◆ Client for Open Enterprise Server For information, see ◆ Section 7.5.4, “Managing the Trustee Rights in the NSS File System,” on page 86) ◆ “rights” in the *OES 2023: NSS File System Administration Guide for Linux*).
UIDs for Linux Access	◆ Use the `nitconfig` tool to configure the Novell Identity Translator (NIT) to manage UIDs for both eDirectory and Active Directory users See “Section 7.2, “NIT (Novell Identity Translator),” on page 58”.
Users and Groups	**AD Users and Groups** ◆ Use native AD tools, such as the Microsoft Management Console (MMC) **eDirectory Users and Groups** ◆ Use iManager

7 NSS AD Utilities and Tools

This section describes the software and tools for managing NSS AD.

- Section 7.1, “List of NSS AD Supported Tools,” on page 57
- Section 7.2, “NIT (Novell Identity Translator),” on page 58
- Section 7.3, “novell-ad-util,” on page 65
- Section 7.4, “NURM (OES User Rights Map),” on page 71
- Section 7.5, “NFARM (OES File Access Rights Management),” on page 83
- Section 7.6, “FTP (Pure-FTPd) and OES for AD Users,” on page 97

7.1 List of NSS AD Supported Tools

The following tools are either new or enhanced to manage NSS AD Support in OES 2015 or later. A brief description of the NSS AD functionality follows each tool name.

- **Auditing Client Logger (VLOG):** Audit all file operations of AD users. For more information, see *OES 2023: NSS Auditing Client Logger (VLOG) Utility Reference*.
- **iManager:** Use the Storage plug-in to manage AD support on NSS pools and volumes.

  NOTE: iManager cannot be used to manage AD users and groups or their trustee rights on NSS resources.

  For more information, see “iManager and Storage-Related Plug-Ins” in the *OES 2023: NSS File System Administration Guide for Linux*.
- **metamig:** Save and restore NSS file system trustee, user quota, and directory quota metadata for AD trustees.

  For more information, see “iManager and Storage-Related Plug-Ins” in the *OES 2023: NSS File System Administration Guide for Linux*.
- **nBackup:** Back up and restore the NSS AD data and metadata.

  NOTE: The nbackup utility can be run only as an eDirectory user. Active Directory users cannot run this utility.

  For more information, see “Backup Applications” in the *OES 2023: Storage Management Services Administration Guide for Linux*.
- **nitconfig:** Specify and configure how the Novell Identity Translator (NIT) handles UID assignments for Active Directory users and groups.

  For more information, see Section 7.2, “NIT (Novell Identity Translator),” on page 58.

- **OES User Rights Map (NURM):** Apply the NSS trustee rights of eDirectory users, groups, and containers to Active Directory users and groups. The basic process is as follows:

  1. Create a proposed mapping between the eDirectory to Active Directory objects using a common name or other fields.
  2. If needed, modify the proposed mapping and then save it.
  3. Apply the mapping to assign rights to corresponding AD users.

  For more information, see Section 7.4, “NURM (OES User Rights Map),” on page 71.

- **OES Files Access and Rights Management (NFARM):** Manage the rights and quotas of AD users or groups on Storage Services (NSS) resources.

  For more information, see Section 7.5, “NFARM (OES File Access Rights Management),” on page 83.

- **NRM:** Manage AD user connections and open files, and generate inventory reports for AD users.

  For more information, see *OES 2023: OES Remote Manager Administration Guide*.

- **NSSCON:** Using new NSS commands, upgrade NSS pool media to support Active Directory, AD-enabling NSS volumes, and so on.

  For more information, see the pool and volume sections in “NSS Commands” in the *OES 2023: NSS File System Administration Guide for Linux*.

- **NSS Rights Utility:** Specify NSS trustee rights for AD users and groups.

  The trustee information is saved in the file and directory metadata on the NSS volume and works seamlessly with NetWare if the volume is moved to a NetWare server.

  For more information, see “rights” in the *OES 2023: NSS File System Administration Guide for Linux*.

- **NSS Quota (nssquota) Utility:** Set, get, or clear the AD user and group quotas on NSS volumes and files.

  For more information, see “nssquota” in the *OES 2023: NSS File System Administration Guide for Linux*.

- **NSS Change Owner (nsschown) Utility:** Manage ownership of NSS resources for AD users.

  For more information, see “nsschown” in the *OES 2023: NSS File System Administration Guide for Linux*.

- **NSSMU Utility:** Update NSS pools to support AD and AD-enabled NSS volumes.

  For more information, see “NSS Management Utility (NSSMU) Quick Reference” in the *OES 2023: NSS File System Administration Guide for Linux*.

7.2 NIT (Novell Identity Translator)

The Novell Identity Translator (NIT) is a new service introduced in OES 2015 as explained in the following sections:

- Section 7.2.1, “A New NSS Authorization Model,” on page 59
- Section 7.2.2, “Not All Users Have UIDs by Default,” on page 59
- Section 7.2.3, “Ensuring that Your CIFS-NSS Users Have UIDs,” on page 59
- Section 7.2.4, “Which OES Components Rely on NIT,” on page 60

- Section 7.2.5, “What NIT Does,” on page 60
- Section 7.2.6, “Prerequisites,” on page 61
- Section 7.2.7, “NIT Components,” on page 61
- Section 7.2.8, “NIT Log Files,” on page 61
- Section 7.2.9, “Interactions With eDirectory and Active Directory,” on page 62
- Section 7.2.10, “How NIT Works,” on page 62
- Section 7.2.11, “Active Directory users:,” on page 63
- Section 7.2.12, “eDirectory users:,” on page 63
- Section 7.2.13, “Task FAQ,” on page 63
- Section 7.2.14, “Administrative Access Restrictions,” on page 64
- Section 7.2.15, “Performance and Tuning,” on page 65

7.2.1 A New NSS Authorization Model

Beginning with OES 2015, a new authorization model has been included for CIFS-user access to NSS volumes.

The new model requires that eDirectory and Active Directory (AD) users all have unique User IDs (UIDs).

7.2.2 Not All Users Have UIDs by Default

- **eDirectory:** LUM-enabled eDirectory users have UIDs; non-LUM-enabled eDirectory users do not.
- **Active Directory:** Generally speaking, AD users don’t have UIDs, but AD can be configured to assign the `uidNumber` attribute to users when required.

7.2.3 Ensuring that Your CIFS-NSS Users Have UIDs

The Novell Identity Translator (NIT) lets you ensure that all users requiring NSS authorization have the required UIDs.

- **eDirectory:** When NIT is properly configured, all eDirectory users can access NSS using CIFS, as summarized in Table 7-1.

Table 7-1 *NIT Guarantees UIDs for All eDirectory Users*

User UID Status in eDirectory	What NIT Does
LUM-enabled user	Retrieves the UID from eDirectory
Non-LUM-enabled user	Generates a UID within the specified UID range

- **Active Directory:** If needed, you can configure NIT to simply retrieve and pass along UIDs that are set in Active Directory by deselecting the **Generate UIDs for AD Users** option when you Configure the NSS AD Support service. However, you must then ensure that all AD users who need access to NSS through CIFS have the `uidNumber` attribute set on their AD account. The caveats associated with the **Generate UIDs for AD Users** option are summarized in Table 7-2.

Table 7-2 *NIT Can Guarantee UIDs for Active Directory Users*

UIDs in Active Directory	Generate UIDs for AD Users Option Status	What NIT Does
The `uidNumber` attribute is set for some or all AD users. Those users have a UID number in Active Directory.	Enabled	Generates UIDs within the specified UID range for all AD users needing NSS access. The `uidNumber` attribute in Active Directory is ignored.
	Disabled	Retrieves the `uidNUmber` from Active Directory when available. Users without a `uidNumber` cannot access NSS.
The `uidNumber` attribute is not set for any AD users. No AD users have a UID number in Active Directory	Enabled	Generates UIDs within the specified UID range for all AD users needing NSS access.
	Disabled	No users can access NSS because none of them has a UID.

7.2.4 Which OES Components Rely on NIT

NIT is used as an infrastructure component by various OES services, including CIFS, NSS, and SMS.

7.2.5 What NIT Does

NIT does the following:

- Dynamically generates UIDs for non-LUM-enabled eDirectory users so that they can access NSS resources on Linux.
- As specified in the `nitd.conf` file, either retrieves or dynamically generates UIDs for Active Directory users so that they can access NSS resources on Linux.
- Provides user and group IDs and other details such as SID, samAccountName, GUID for AD identities and FQDN, GUID details for eDirectory identities to services like NSS, CIFS, and SMS.
- Is backward-compatible and co-exists with Linux User Management (LUM).
- Maintains all of the users information in an AD forest where the OES server's computer object is located.
- Ensures uniqueness of User IDs for all the users across eDirectory and Active Directory users and groups accessing an OES server.

NOTE: The UIDs distributed by NIT are server-specific. They are not stored in eDirectory or Active Directory, and they are not visible to Linux services.

7.2.6 Prerequisites

The following are required for NIT to service Active Directory users and groups:

DNS

- **Domain Controller and Global Catalog Server Discovery:** DNS entries for all the Domain Controllers and Global Catalog Servers must exist in order for NIT to detect which of them are closest and then retrieve the required AD user information. Ensure to provide the complete DNS name of the OES CIFS server.
- **SRV Records:** The DNS should contain the SRV entries for the Domain Controllers, Global Catalog servers and KDC servers in the OES joined forest and other trusted forests.

Kerberos

For external forest trusts, “Kerberos Forest Search Order (KFSO)” should be enabled for Windows clients to connect an OES CIFS server. For more information, see Configuring AD Server to Support Kerberos Authentication for External Forest Users Using CIFS Client in the OES 2023: OES CIFS for Linux Administration Guide.

7.2.7 NIT Components

NIT contains the following components:

- **nit daemon:** Serves requests from CIFS, NSS, SMS, and other OES services to map and resolve eDirectory and Active Directory user identities as applicable.
- **nitconfig utility:** Lets administrators configure NIT in a terminal prompt by adding and modifying configuration parameters. The `nitconfig` utility changes the `/etc/opt/novell/nit/nitd.conf` file based on the parameters entered.
- **NIT configuration file:** `/etc/opt/novell/nit/nitd.conf`.

  Each entry occupies a single line in the file. Lines that are blank, or that start with a pound sign (#), are ignored.

IMPORTANT: If you change the NIT UID range, either manually or using the `nitconfig` utility, you must restart the server.

7.2.8 NIT Log Files

NIT actions are logged in the following locations:

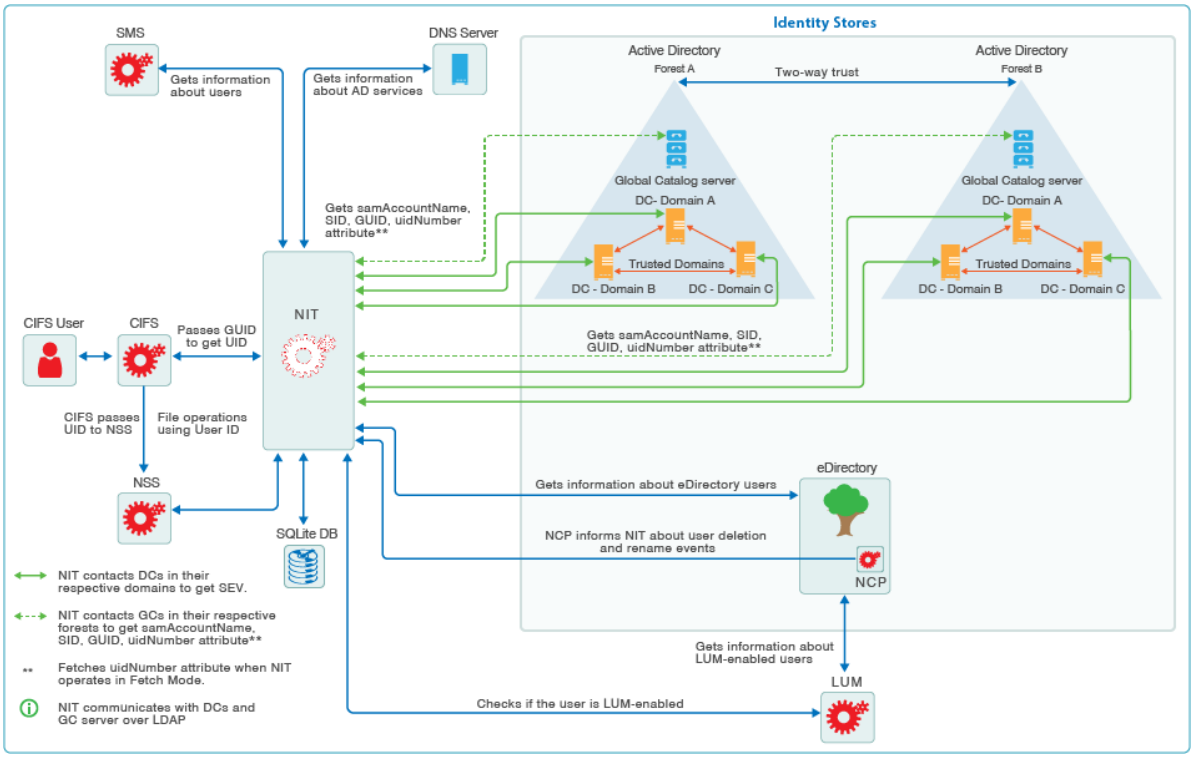
- **NIT log:** `/var/opt/novell/logs/nit/nit.log`
- **nitconfig log file:** `/var/opt/novell/log/nit/nitconfig.log`

7.2.9 Interactions With eDirectory and Active Directory

NIT interacts with LUM, NCP, the AD Global Catalog Server, and Domain Controllers to retrieve and map user information.

7.2.10 How NIT Works

Figure 7-1 *NIT - overview*



NIT supports two identity stores:

- Active Directory

  and

- eDirectory

NIT can run in two modes:

- Support only eDirectory
- Support eDirectory and Active Directory

You can configure this through `nitconfig` by changing the value of `ad-mode` parameter. If you set the value to `yes`, then NIT supports eDirectory and Active Directory. If you set it to `no`, then NIT supports only eDirectory.

7.2.11 Active Directory users:

For Active Directory users, NIT can be configured to run in one of two modes:

- **Generate Mode:** NIT generates and uses its own UID numbers. Even if the Active Directory users have the UID numbers populated, those are not used by NIT.

  or

- **Fetch Mode:** NIT only retrieves UID numbers that are available in Active Directory. If a UID is not set for a particular user, that user cannot access NSS resources.

  If you are configuring NIT in fetch mode for Active Directory users, ensure that the Active Directory users who require access to NSS file systems have UID numbers set in Active Directory.

  You must add the `uidNumber` attribute explicitly to the Global Catalog server because it is not part of the default attributes.

  For more information about replicating UID numbers to the Global Catalog server, refer to the Microsoft Support website.

By default, NIT runs in generate mode where UID numbers are dynamically generated for Active Directory users within the range that you specify in the NIT configuration.

7.2.12 eDirectory users:

For eDirectory LUM-enabled users, NIT obtains the UID number that is already available in eDirectory. NIT automatically creates UIDs for non-LUM-enabled users from the UID range that you specify either directly in `nitd.conf` or through the `nitconfig` utility.

7.2.13 Task FAQ

How do I set UID ranges?

You can set the UID ranges through YaST as part of the OES installation.

You can also set and manage UID ranges using the `nitconfig` utility after the NIT service is configured as part of OES installation.

How do I estimate UID ranges?

Estimate the number of users who might access the server, and then set a UID range that is double that number. Ensure that these ranges do not overlap with the LUM ranges and Linux UID ranges, if present.

How long are UIDs valid?

The UIDs are valid until the OES system is rebooted. However, the UIDs are retained when the NIT service restarts.

Are the UIDs unique?

UIDs generated are unique within each server's environment, including the Identity stores (eDirectory and Active Directory) and the local file systems (both Linux and POSIX).

What happens if a cluster resource is moved?

When a cluster resource is mounted on a different cluster node, UIDs are automatically generated for new user connections on the new node. UID management and generation is specific to each cluster node (OES 2018 server). There is no NIT configuration or activity at the cluster level.

How do I manage NIT?

To start, stop, and restart the NIT service, use these command options:

```
rcnovell-nit status | stop | start | restart
```

To configure and change NIT settings, use the `nitconfig` utility.

IMPORTANT: If you change the NIT UID range, you must restart the server.

What is cache and SQLite DB?

NIT stores eDirectory and Active Directory user information, GUID to UID mapping information and SID to GUID mapping information in non-persistent in-memory cache.

NIT stores GUID to UID (UIDs generated by NIT for non LUM-enabled eDirectory and Active Directory users) mapping information in `/var/opt/novell/nit/db/.g_i_info` SQLite DB file, and SID to GUID mapping information in `/var/opt/novell/nit/db/.s_g_info` SQLite DB file. The information stored in SQLite DB files are persistent across NIT restarts.

On a server reboot, the in-memory cache information is cleared and the `.g_i_info` SQLite DB file is deleted.

When the NIT daemon is restarted, the in-memory cache is cleared and NIT rebuilds GUID to UID mapping information and SID to GUID mapping information into cache by reading from the SQLite DB files.

In addition, only the user information in the in-memory cache is cleared once in 8 hours and the GUID to UID and SID to GUID mapping information remain unaltered.

7.2.14 Administrative Access Restrictions

When an OES server is joined to an Active Directory domain, by default, members of the Domain Admins group will have Supervisor rights over all the volumes that are enabled with Active Directory identities flag.

You can override this default functionality by configuring a group of your choice. Because the group has full control over the Active Directory enabled volumes, add users with caution.

If NIT could not identify the configured group from Active Directory, it falls back to the default behavior.

Whenever you change the Active Directory supervisor group, do the following:

1. Restart the NIT daemon by running the `rcnovell-nit restart` command at the terminal console.
2. Restart the CIFS service by running the `rcnovell-cifs restart` command at the terminal console.
3. Force the SEV update to occur immediately for all users in the NSS file system by running the `nss /ForceSecurityEquivalenceUpdate` command at the `nsscon` prompt.

7.2.15 Performance and Tuning

- **ad-gc-handles:** NIT interacts with the Global Catalog servers to fetch Active Directory user and group information. By default, NIT establishes 10 connections with the GC server. Based on the number of users, increase this number to improve the file access response time.
- **hash-size:** NIT caches eDirectory and Active Directory user information in hash tables. By default, the size is configured to 211. This can be increased to a maximum of 1:10. For example, for 20,000 users the hash size will be a prime number close to 2048.

  NIT stores the user cache information in the following SQLite DB files: `/var/opt/novell/nit/db/.g_i_info` and `/var/opt/novell/nit/db/.s_g_info`.
- **UID Start and End Range:** Changing the UID start and end ranges requires a system reboot.

7.3 novell-ad-util

The Novell AD Utility (`novell-ad-util`) lets you do the following:

- Join an OES server/cluster node or a cluster resource to an AD domain.
- Remove an OES server/cluster node or cluster resource from an AD domain.
- Manage the Kerberos keytab files of OES servers/cluster nodes and cluster resources as required for authentication within the domain.

The YaST installation component that lets you join an OES server/cluster node to an AD domain as part of configuring NSS AD support, leverages `novell-ad-util` in the background.

7.3.1 novell-ad-util Command Line Utility

`novell-ad-util` joins an OES server/cluster node or a cluster resource to an AD domain, and manages the Kerberos keytabs of those components.

Syntax

`novell-ad-util <activity> <optional parameters>`

Usage Options

Primary Activity

--join

Joins the current host or cluster resource to the Active Directory domain.

--leave-domain

Disjoins the current host or cluster resource from the Active Directory domain by deleting the computer object from AD and flushes all entries from the keytab, including samAccountName.

NOTE: To execute the `--join` or `--leave-domain` commands, the user's Credential Cache should have sufficient rights to create or delete an object in Active Directory.

--validate-container

Checks if the container exists in the domain specified. It must be followed by the `--context` option.

--purge <number>

Purges the keytab entries, retaining only the last specified number of key versions.

If this command is executed without the `--cluster-resource` option, key tab entries of the host are purged.

If this command is executed with `--cluster-resource` option, key tab entries of the cluster resource are purged.

--reset

Resets the password, adds service principals if any, and updates all the corresponding entries in the keytab.

--auto-reset

Resets the password, adds service principals if any, and updates all the corresponding entries in the keytab, if the password age is more than 30 days.

--online

This command is used for cluster resources. It must be followed by the `--cluster-resource` option. This command will merge the keys residing in the keytab files of the volumes with the default keytab of the node.

--offline

This is used generally for cluster resources. Must be followed by the `--cluster-resource` option. When a cluster resource goes offline in a node during migration, this command will copy all they keys related to the cluster resource to all the available volumes' keytab from the node's default keytab.

--create-object

Creates a computer object in a non-default realm (a realm other than the one to which the host or cluster resource is joined) and updates the keytab entries. To create a computer object for a cluster resource, use this option with --cluster-resource.

--delete-object

Deletes a computer object that is created using --create-object along with the keytab entries. To delete a computer object for a cluster resource, use this option with --cluster-resource.

NOTE: To execute --create-object or `--delete-object`, the user's Credential Cache should have sufficient rights to create or delete an object in Active Directory.

Optional Parameters

--service-principal <service_name>

Creates a service principal for the associated account. For example, *<service_name>/<hostname>.<domain_name>@<DOMAIN_NAME>*.

--domain-name <domain_name>

Use the domain name specified instead of parsing the krb5 file to retrieve the domain name.

--context

Allows you to join your machine to a specific context of Active Directory (Default is CN=Computers.)

--pre-created-object [yes/no]

Allows you to join your machine to a pre-created computer object in the Active Directory. (Default is no.)

--realm-name <realm_name>

Allows you to specify the non-default realm for the multi-realm operation such as --create-object or `--delete-object`. This option is mandatory for multi-realm operations.

--description <Description>

Allows you to specify the description for a computer object. Must be used with the option --join, --create-object, or `--reset`. If this option is not specified, the default description 'Open Enterprise Server' or 'Open Enterprise Server Cluster Resource' is used.

When this option is used with `--reset`, if the computer account (SELF) does not have sufficient rights, it fails to set the description. By default, the computer account (SELF) does not have WRITE permission on the description attribute of its object. The administrator can manually provide the WRITE permission on the description attribute at the container level for such computer account

--cluster-resource <virtual server_FDN_eDir_format>

Joins or updates the current cluster resource to the Active Directory.The object will be created as the NETBIOS name of the cluster resource with

- **samAccountName:** *<NetBIOS_NAME>$*
- **service principal:** *host/<NetBIOS_NAME>.<domain_name>@<DOMAIN_NAME>*.

If used with --join or --reset, it also updates the keytab in

- Each available volume associated with that resource in <mount_path>/VOL_NAME/ ._NETWARE/vol.keytab
- The default keytab

To find the virtual server FDN for the cluster resource in eDirectory format:

At the command prompt, execute the following commands.

1. `cluster resources` to get the list of cluster resources.
2. `cat /var/opt/novell/ncs/<cluster_resource>.load`, for example, `cat /var/opt/novell/ncs/NSSAD64_SERVER.load`.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuncs
exit_on_error nss /poolact=NSSAD64
exit_on_error ncpcon mount BLR716993_VOL2=253
exit_on_error add_secondary_ipaddress 192.168.100.10
exit_on_error ncpcon bind --ncpservername=NSS64VM-NSSAD64-SERVER --
ipaddress=192.168.100.10
exit_on_error novcifs --add '--vserver=".cn=NSS64VM-NSSAD64-
SERVER.o=novell.t=NSS64VM-TREE."' --ip-addr=192.168.100.10
exit 0
```

3. Identify the virtual server FDN for the cluster resource ".cn=NSS64VM-NSSAD64-SERVER.o=novell.t=NSS64VM-TREE." in the line exit_on_error novcifs --add '--vserver=".

--pooldn <cluster_pool_FDN_eDir_Format>

This can be used instead of cluster_resourceFDN.

Examples

novell-ad-util --join --domain-name EXAMPLE.COM --service-principal cifs

If your server name is *oes2018_server.example.com*, executing this command will create an account oes2018_server with

- **samAccountName:** *oes2018_server$*
- **Service Principals:** *host/oes2018_server.example.com@EXAMPLE.COM*, *cifs/oes2018_server.example.com@EXAMPLE.COM*, and *cifs/oes2018_server@EXAMPLE.COM*

Then it associates those principals with the computer account.

It also updates the default keytab, `/etc/krb5.keytab` and `/etc/krb5.conf` files.

novell-ad-util --join --cluster-resource .cn=CLUSTER-OES2018-POOL-SERVER.o=novell.t=NSSAD_CLUSTER. --domain-name EXAMPLE.COM --service-principal cifs

If your cluster resource eDirectory object is *.cn=CLUSTER-OES2018-POOL-SERVER.o=novell.t=NSSAD_CLUSTER.* and it's NetBIOS name is *cluster2018*, executing this command will create an account cluster2018 (NetBIOS name) with,

samAccountName: *cluster2018$*

Service Principals: *host/cluster2018.example.com@EXAMPLE.COM*, *cifs/cluster2018.example.com@EXAMPLE.COM*, and *cifs/cluster2018@EXAMPLE.COM*.

and associates those principals with the cluster account.

If this cluster resource has volumes, VOL1 and VOL2 mounted on `/media/nss`, it updates the following:

- The default keytab `/etc/krb5.keytab`
- The keytab files in the volumes
  - /media/nss/VOL1/._NETWARE/vol.keytab
  - /media/nss/VOL2/._NETWARE/vol.keytab
- The kerberos configuration file `/etc/krb5.conf`

novell-ad-util --join --pooldn .cn=CLUSTER_OES2018_POOL.o=novell.t=NSSAD_CLUSTER. --domain-name EXAMPLE.COM --service-principal cifs

Executing this command will join the cluster resources as explained in the previous example.

novell-ad-util --leave-domain --domain-name EXAMPLE.COM

Executing this command will disjoin the current host from the Active Directory domain.

novell-ad-util --leave-domain --cluster-resource .cn=CLUSTER-OES2018-POOL-SERVER.o=novell.t=NSSAD_CLUSTER. --domain-name EXAMPLE.COM

Executing this command will disjoin the cluster resource specified from the Active Directory domain.

How do I remove stale entries of keytab for unjoined cluster resources on all cluster nodes in the cluster?

When you disjoin a cluster resource from an Active Directory domain, novell-ad-util removes the keytab entries of that resource from the default keytab file, `/etc/krb5.keytab`, and deletes the volume keytab file. For example, `/media/nss/vol1/._NETWARE/vol.keytab` on the node where the resource is running.

Before disjoining the resource, if you have migrated it to other cluster nodes, all the cluster nodes where the resource is migrated will have the default keytab entires.

When you disjoin the cluster resource, the default keytab entries for that specific cluster node and the volume keytab entries will be removed. However, the default keytab entries will still be seen on those nodes where the resource was migrated.

To remove the stale entries, execute the following command respectively all nodes other than the node that you used for the resource disjoin:

```
novell-ad-util --purge 0 --cluster-resource <cluster dn> --domain-name <domain name>
```

This command removes the keytab entries of the cluster resource <cluster dn> specified; it will not remove the volume keytab file.

novell-ad-util --validate-container --context CN=OES2018Servers --domain-name EXAMPLE.COM

Validates the container OES2018Servers in the domain example.com.

novell-ad-util --purge 2

Removes keytab entires of the host from the default keytab file, retaining only the last two key versions. For example, if key versions 2,3,4,5 exist in the keytab file, executing this command will purge versions 2 and 3, and retain versions 4 and 5.

novell-ad-util --purge 2 --cluster-resource .cn=CLUSTER-OES2018-POOL-SERVER.o=novell.t=NSSAD_CLUSTER.

Removes keytab entires of the cluster resource specified from the default key tab file, retaining only the last two key versions. For example, if key versions 2,3,4,5 exist in the key tab file, executing this command will purge versions 2 and 3, and retain versions 4 and 5.

novell-ad-util --purge 0 --cluster-resource .cn=CLUSTER-OES2018-POOL-SERVER.o=novell.t=NSSAD_CLUSTER.

Removes all the keytab entries of the cluster resource specified from the default key tab file.

novell-ad-util --join --domain-name EXAMPLE.COM --context cn=OES2018Servers --pre-created-object yes --service-principal cifs

Joins this host to the Active Directory domain, provided the computer object for this host should already exist in Active Directory. The name of the pre-created object should be the same as the NetBIOS name of the server object.

novell-ad-util --create-object --service-principal cifs --realm-name TESTAD.COM --cluster-resource .cn=CLUSTER16-CLUS-POOL1-SERVER.o=novell.t=EDIR_CLUS16.

Creates a computer object of a cluster resource in a non-default realm TESTAD.COM and updates the keytab entries.

novell-ad-util --delete-object --realm-name TESTAD.COM --cluster-resource .cn=CLUSTER16-CLUS-POOL1-SERVER.o=novell.t=EDIR_CLUS16.

Deletes the computer object of a cluster resource from the non-default realm TESTAD.COM.

novell-ad-util --create-object --service-principal cifs --realm-name TESTAD.COM --cluster-resource .cn=CLUSTER16-CLUS-POOL1-SERVER.o=novell.t=EDIR_CLUS16. --description "OES TEST OBJECT"

Creates a computer object of a cluster resource in a non-default realm TESTAD.COM and updates the description as OES TEST OBJECT.

Files

/etc/krb5.conf

Stores Kerberos configuration.

/etc/krb5.keytab

Default keytab file that contains Service Principals of the OES server/cluster node or cluster resource.

/var/log/novell-ad-util/novell-ad-util.log

Stores the log information.

/etc/cron.daily/ad-util-auto-update

Sets the cron job to execute the `ad-util-auto-update` script every day and checks whether the password age is more than 30 days. If yes, resets the password of a node computer account and all cluster resource computer accounts. It ensures only two sets of key versions are present in the keytab files and also, the default keytab files and volume keytab files are in sync.

/etc/cron.daily/ad-util-auto-update --force-reset

Forcefully reset the password of a node computer account and all cluster resource computer accounts. For testing purpose, you can manually execute this command.

Help Options

--help

Displays the help information commands and syntax, and then exits.

7.4 NURM (OES User Rights Map)

The OES User Rights Map (NURM) utility is used by administrators to map the Access Control List (ACL) of NSS resource that is owned by an identity in eDirectory to an identity in Active Directory. It maps the users and groups from eDirectory to Active Directory using a common name or any other field that is selectable by the tool. With this utility, the administrators can:

- **Create User Maps:** Map eDirectory and Active Directory users and groups.
- **Leverage Existing IDM-based User Maps:** Leverage NetIQ Identity Manager 4.5 or later maps that are created using IDM Designer (but not the IDM iManager plug-in).
- **Map User Rights:** Assign rights to Active Directory users on NSS resources.
- **View Rights:** View the rights of Active Directory and eDirectory users on a given volume.
- **Synchronizing Rights:** Synchronize the rights of Active Directory and eDirectory users using the `user-rights-map` command line utility.

- Section 7.4.1, “Prerequisites,” on page 71
- Section 7.4.2, “Accessing OES User Rights Map Utility (NURM),” on page 71
- Section 7.4.3, “Mapping Users,” on page 72
- Section 7.4.4, “Mapping Rights,” on page 75
- Section 7.4.5, “Viewing Rights,” on page 76
- Section 7.4.6, “Changing the NURM Settings,” on page 77
- Section 7.4.7, “NURM Command Line Utility,” on page 78

7.4.1 Prerequisites

- Ensure that the universal password is enabled for the eDirectory user who is accessing NURM. This utility uses CIFS to fetch the volume information. Hence, when a user who is not universal-password-enabled accesses NURM, the volumes are not listed under the **View Rights and Map Rights** pages. For more information on enabling Universal Password Policy, see“CIFS and Universal Password” in the *OES 2023: OES CIFS for Linux Administration Guide*.
- The eDirectory user managing NURM must have read and write access on the `/_admin/Manage_NSS/manage.cmd`.
- Ensure that CIFS user context is configured for the eDirectory user who is accessing NURM. For more information, see “Configuring a CIFS User Context” in the *OES 2023: OES CIFS for Linux Administration Guide*.
- If you are to use NURM in an environment where eDirectory and Active Directory are synchronized using NetIQ IDM, ensure that `DirXML-ADContext` attribute is populated in eDirectory server.

7.4.2 Accessing OES User Rights Map Utility (NURM)

Along with the installation and configuration of NSS AD, the NURM utility gets installed.To access the NURM:

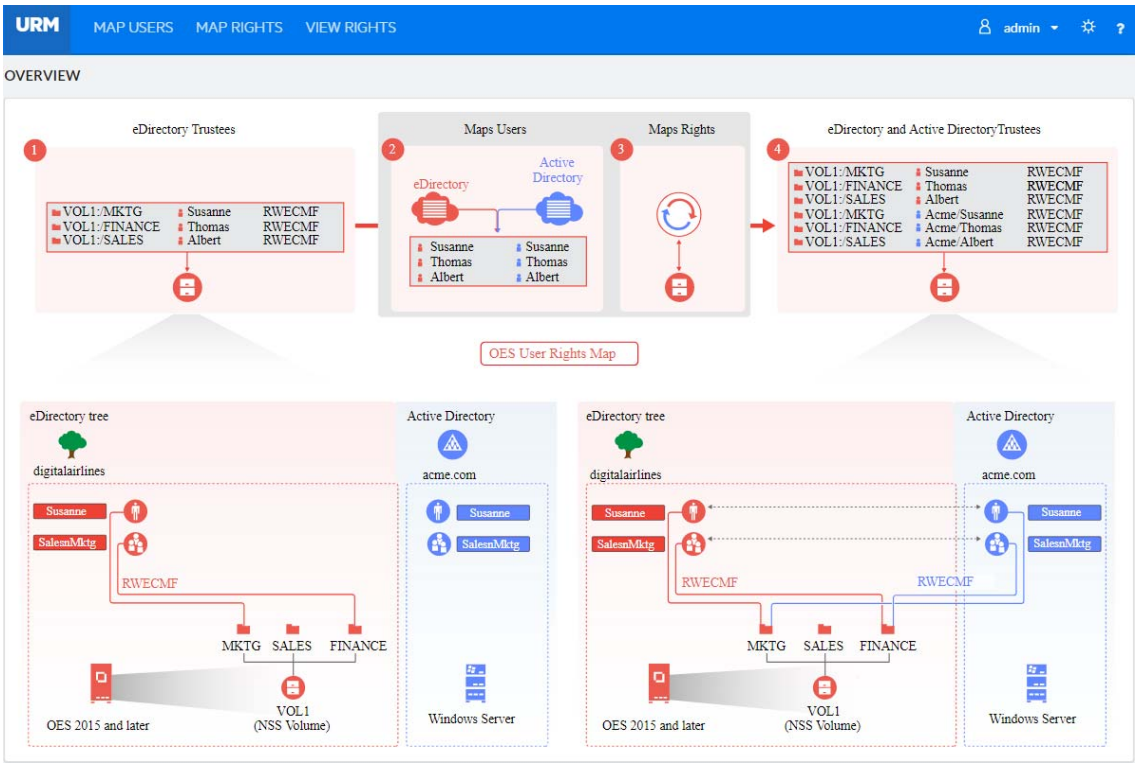
1 Open the OES server welcome page, then click **Management Services > OES User Rights Map**.

OR

Point your browser to https://*<OES server IP address or the host name>*/storm.

2 Specify the user name or the FQDN of the eDirectory administrator in the **User Name**, specify the password, then click **Login**.

The NURM welcome page should look similar to the following:



NURM is also available as a command line utility (`user-rights-map`). For more information on the CLI utility, see Section 7.4.7, “NURM Command Line Utility,” on page 78.

7.4.3 Mapping Users

In an NSS AD environment, OES servers are joined to an Active Directory domain to provision AD users and groups native NSS resources access. To aid this, identities from Active directory will have to be mapped with identities on eDirectory and assigned the same rights as that of the eDirectory identities. NURM helps in creating this identity map, which is called a “user map”. User maps are used to assign rights to AD identities on the NSS resources.

Using the Map Users feature, administrators can do the following:

- Create new user maps: Map eDirectory and Active Directory (AD) users and groups.
- Import user maps
- Export user maps
- Refresh user maps
- Delete user maps

Before creating user maps, ensure that you are connected to an AD server.

Connecting to an Active Directory Server

Whenever an authentication is required, **Connect to Active Directory** pop-up window is displayed.

For example: In Map Users page, click + icon and specify the following details, then click **Connect** to connect to the target AD server.

- **User Name:** Specify the AD Administrator user name or the FQDN.
- **Password:** Specify the AD Administrator password.
- **Domain Name:** Specify the realm of the AD domain.
- **Port:** Specify the port with which you would like to connect to the AD server. If you would like this connection to be secure, select Use SSL. Some of the standard LDAP ports for Active Directory are 389, 636, 3268, and 3269.

NOTE: ◆NURM supports multiple AD forests. Login to the respective forest before generating the user map.

- When connecting to Active Directory, specify the credentials of the respective domain (PDC or CDC) where the users or groups exists.

Creating a New User Map

1 Click +, then specify the following details:

- **Match Type:** Select an object mapping (user to user, group to group, or container to group). In the **Target Matching Pattern**, specify the wildcard-based search criteria.

  For example, if you want to match a group from the source identity store with a group on the target identity store that differs in naming conventions, you can use the **Target Matching Pattern**.

  For example, assume that you have the following groups on the source identity: `eng-group-acme`, `sales-group-acmeUS`, and so on; and `technology-acme`, `sales-acmeUS`, and so on in the target identity. In the **Target Matching Pattern**, specifying `*-acme` finds the match from eng-group-acme and technology-acme groups.

- **LDAP Attributes:** Select Common Name to Common Name (CN to CN), Common Name to SAM-Account-Name (CN to SAM), or Custom Attributes matching criteria.

  If you choose custom attributes, you will have to specify the eDirectory and Active Directory object attributes.

  Examples of eDirectory object attributes include User Name (uid), Common Name (cn), Last Name (sn), First Name (givenName), Full Name (fullName), and Internet E-mail address (mail).

  Examples of Active Directory object attributes include Common Name (cn), Full Name (name), SamAccount Name (sAMAccountName), First Name (givenName), Last Name (sn), Display Name (displayName), Internet E-mail address (mail), UserPrincipleName.

- **eDirectory Context:** Specify or browse and select the eDirectory tree search base context. The **Search Subtree** option is enabled by default.
- **Active Directory Context:** Specify or browse and select the AD server context. The **Search Subtree** option is enabled by default.

2 Click **Show** to generate and view the user map. To propose a usermap of your choice, go to Step 3 on page 74.

OR

Click **Save** to generate and store the user map on the server.

NOTE: If you choose to store the user map on the server, you can validate and modify the user map only after it gets listed in the Map Users page.

---

3 Validate the user mapping. If you need to modify any user mapping:

3a Click on selected Active Directory context and browse to the appropriate AD server context, then click **Select**.

3b To replace or add an AD user in the proposed user map, select a row in the proposed user map, then click .

3c To remove a user from the proposed user map, click . To undo the deletion, click .

3d Click **Save Map** to save all the changes.

TIP: • To modify an existing user mapping, click the user map name in the Map Users page, then follow the instructions in Step 3 on page 74.

- Sorting: Click icon next to **Sort By** to sort the user map based on the Name, Type, eDirectory Context, and Active Directory Context.

Importing a User Map

1 Click , then select the user map XML file using the **Browse** button.

2 Specify an appropriate name for the user map, then click **Import**.

Exporting a User Map

Select the user map of your choice, click , to download the user map file.

Refreshing a User Map

If you feel that the mapping have changed since the time you have created a user map, you could refresh them using the same conditions that were used while creating them.

To refresh an old user map, go to the desired user map and then click . If there are any differences since the time they were created, those entries are highlighted with the icon. If you would like to revert changes, click **Revert**. After verifying the changes, click **Save Map**.

If the user map is not modified for a time interval specified in the **Usermap Refresh Interval (days)**, a 'Refresh Required' tag is displayed on the user map. For more information, see "Changing the NURM Settings" on page 77.

If scheduled refresh on the user map is enabled, then the 'Last Updated: date and time' tag is displayed on the user map. For more information on user map scheduled refresh, see "Usermap Settings" on page 78.

To view the modified user maps based on the scheduled refresh time, click **SHOW SCHEDULED REFRESH LOGS**. You can hover the cursor over the user map name to view the users added or removed from that user map.

Deleting a User Map

Select the user maps that you want to delete, then click .

7.4.4 Mapping Rights

Using this feature, you can map rights to AD users on a specific NSS volume. While doing so, you can choose to remove eDirectory trustees from the NSS file system and migrate the eDirectory IDs (owner, modifier, archiver, metadata modifier, and deletor) to AD users.

To map rights:

1. Click .
2. Select a volume on which you want to map rights to AD users, then select the source of user mapping:
   - **NetIQ IDM:** If you select this option, then directly go to Step 3 on page 75.

     NOTE: When IDM is used, the connection to eDirectory is established with secure SSL port 636. For information on creating user map using IDM, see the NetIQ Identity Manager 4.7 Documentation.
   - **User Map:** If you select this option, choose the appropriate user map name, then click **Show**. The user map is displayed along with the rights that will be assigned to the AD users. You can hide the user map and rights details using the **Hide** button. You can also select multiple user maps and apply rights.
3. Enable the following options as needed:
   - **Apply to Salvage:** Applies rights to AD users on the salvaged files and folders.
   - **Remove eDirectory Trustees:** After assigning AD users as trustees, the eDirectory users will be removed from the NSS file system as trustees.
   - **Migrate IDs:** Assign eDirectory trustee IDs (owner, modifier, archiver, metadata modifier, and deletor) to AD users.
4. Click **Apply**.

In the Map Rights page, you can delete, view status, view logs, and download logs of a mapped rights.

- **Delete:** Select the map rights to be deleted, then click .

  NOTE: After deletion, you can no longer synchronize rights on the volume using the deleted map rights. Resynching of mapped rights is possible only using the `user-rights-map` command line utility
- **View Status:** Select the map rights, then point the cursor to progress to view the updated status of the map rights.

- **View and Download Log:** Select the map rights, click **View** under the **Log** column. The Log Viewer page is displayed, click **Download** to copy the log file.

7.4.5 Viewing Rights

Using this feature, an administrator can view the explicit rights of both eDirectory and Active Directory users on the selected volume. This is the only tool that allows the administrators to view the rights of both AD and eDirectory users in a consolidated view.

To view rights:

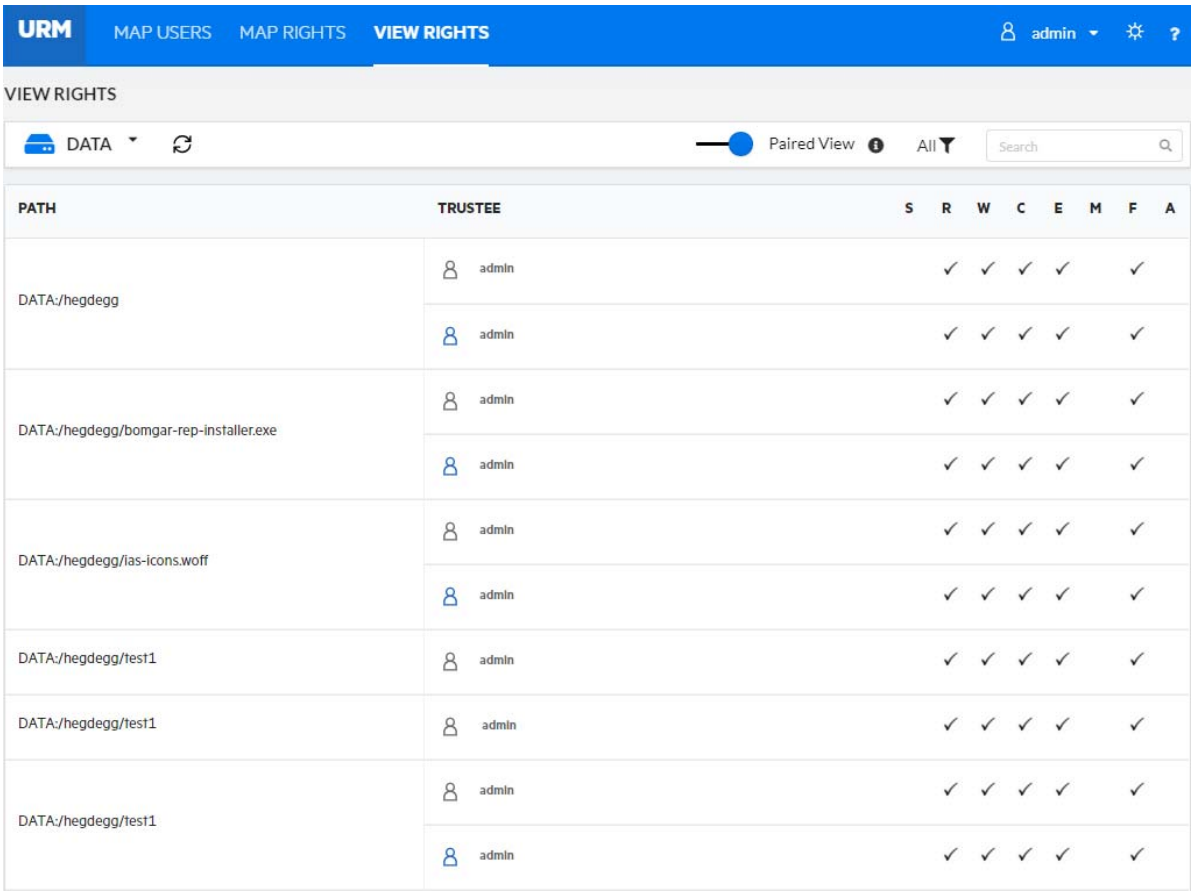
1. Select the volume name from the drop-down list. The explicit rights are displayed along with the path, trustee, and rights information.

   The trustees with the same path are grouped together for better understanding of the view rights.
2. Enable the **Paired View** option to display the eDirectory and Active Directory trustee paired view (with common path). Point your browser to icon to view the mapping (IDM or User Map) selected for viewing rights.

In View Rights page, you can refresh, filter, and search the rights of both eDirectory and Active Directory users.

- **Refresh:** Click icon to view the updated list of explicit rights for both eDirectory and Active Directory users on the selected volume.
- **Filter:** Click icon to filter the view rights based on Users-Mapped, Users-Not Mapped, Groups-Mapped, Groups-Not Mapped, ACL-Matched, and ACL-Not Matched. This filter option is available only for the paired view.
- **Search:** Use this option to display only the required path or trustee name in the View Rights page. This option can be used with the **Filter** to perform a search on the filtered trustees.

TIP: Click the **Trustee** column title to sort the data either in ascending or descending order.



7.4.6 Changing the NURM Settings

Click icon at the top right to go to NURM settings page. It includes:

- **Language:** Select the appropriate language to be displayed on the NURM page.
- **Log Level:** Select the required log level. The supported log levels are Debug, Information, Warning, Error and Fatal. The logs are stored at `/var/opt/novell/log/nurm/user-rights-map.log`.
- **Contextless Login for eDirectory:** Enables or disables the contextless login. By default, this option is enabled. If you would like to always use the FQDN while logging on to NURM, ensure to disable this option.
- **Usermap Refresh Interval (days):** Specify the number of days after which the user maps are considered as old and requires a refresh. For example, when you set the value to 6 days: In Map Users page, a 'Refresh Required' tag is displayed only on those user maps that are not modified for 6 days.
- Select the required mapping to use for View Rights: IDM or User Map. If you have selected User Map, select the appropriate user map name. You can select multiple user maps too.

After changing the NURM settings, click **Save**.

Usermap Settings

This section provides information on the scheduled refresh, which can be used to refresh the user maps automatically if there are changes in the user maps.

It displays:

- Whether the scheduled refresh is enabled or disabled
- If enabled, the time and frequency of the user map refresh

You can enable or disable the `Scheduled Refresh` option only by using the `map-users` command-line utility. For more information, see “map-users” on page 78.

NOTE: Before enabling, ensure that the 'OESCommonProxy' user has 'Read' permission on the **All Attributes Rights** property in the same tree.

7.4.7 NURM Command Line Utility

- “map-users” on page 78
- “user-rights-map” on page 80

map-users

Use this utility to generate a user map after specifying the necessary match type, context and so on.

Syntax

```
map-users
```

```
map-users -u <specify the user map name> -a <eDirectory Username> -w
<eDirectory password> -s <eDirectory Server IP> -p <eDirectory Connection
Port> -l <y|n> -c <eDirectory context> -st <y|n> -t <specify the match type
as user2user, group2group, or container2group> -m <specify the matching
attribute as cn2sam> -A <AD username> -W <AD user password> -S <specify the
AD server IP or domain name> -P <specify the AD server connection port> -L
<y|n> -C <specify the Active Directory context> -ST <y|n>
```

Options

-u, --usermap-file <user map file name>

Specify the name of the user map. After a successful execution of the map-users command the user map file is saved with the name that you specify here.

-a, --user <eDirectory username>

Specify the eDirectory username to connect to NURM.

-w, --password <eDirectory user password>

Specify the eDirectory user password.

-s, --server-ip <eDirectory server IP>

Specify the name IP of the eDirectory server.

-p, --port <eDirectory server connection port>

Specify the port number to be used to connect to the eDirectory server.

-l y|n, --use-ssl-eDir y|n

Enables or disables secure connection. Enable this option if you would like a secure connection to the eDirectory server.

-c, --context <specify the eDirectory server context>

Specify the eDirectory server context. For example, ou=users,o=novell.

-st y|n, --subtree-search y|n

Enables or disables subtree search. Enable this option if you would like to consider all the users in the subtree.

-t, --match-type <specify the match type>

Specify the user match type. For example, user2user, group2group, or container2group.

-m, --matching-attribute <attributes>

Specify the match attributes. For example, cn2sam. As of now only cn2sam is supported.

-sr enable|disable, --scheduled-refresh enable|disable

Enables or disables the schedule refresh of user maps. If you enable this option, it is mandatory to use `--scheduled-refresh-time` with this option.

-srt, --scheduled-refresh-time <MM(0-59) HH(0-23) DD(0-31)>

Specify the time in which the user maps need to be refreshed. This option should be used only with `--scheduled-refresh`.

-A, --USER *<specify the AD user name>*

Specify the fully qualified domain name (FQDN) of the AD user.

-W, --PASSWORD *<AD user password>*

Specify the AD user password.

-S, --SERVER-IP *<specify the AD server IP or domain name>*

Specify the IP address or domain name of the AD server that you would like to connect to.

-P, --PORT <specify the AD server connection port>

Specify connection port with which you would like to connect to the AD server.

-L y|n, --USE-SSL-AD y|n

Enables or disables secure connection. Enable this option if you would like a secure connection to the AD server.

-C, --CONTEXT <specify the AD server context>

Specify AD server context.

-ST y|n, --SUBTREE-SEARCH y|n

Enables or disables subtree search. Enable this option if you would like to consider all the users in the subtree.

-h, --help

Displays the usage information of the command.

Examples

1. For an interactive user map generation, use the following command and follow the on screen instructions:

   ```
   map-users
   ```

2. To map users by providing all the arguments:

   ```
   map-users -u mkt-usr-map -a root -w pa55word -s 192.168.1.1 -p 636 -l y
   -c ou=users,o=mkt -st y -t user2user -m cn2sam -A
   cn=administrator,cn=users,dc=acme,dc=com -W Pa55word@@ -S 192.168.1.2 -
   P 636 -L y -C cn=users,dc=acme,dc=com -ST y
   ```

   This command creates a user map with the following details:

   - Saves the user map as “mkt-usr-map”
   - Connects to the eDirectory server (192.168.1.1) with root credentials, context as ou=users,o=mkt, match type as user to user, matching attributes as CN to SAM, and searches the entire subtree while generating the user map. The connection type used is SSL using port 636.
   - Connects to the AD server (192.168.1.2) using the administrative credentials, context as cn=users,dc=acme,dc=com, and searches the entire subtree while generating the user map. The connection type used is SSL using port 636.

3. To schedule a refresh of all user maps available in the OES tree:

   ```
   map-users --scheduled-refresh enable --scheduled-refresh-time "30 9 4"
   ```

   This command schedules a cron job (scheduled refresh) to execute at 9:30 AM on every 4 days.

user-rights-map

Use this utility to map the rights of the mapped eDirectory and Active Directory users, groups, and containers. The mapped rights information is stored in a file and assigned an ID. Using this id, you can synchronize the rights of the users.

The **User Rights Map** GUI runs as a `wwwrun` user and `user-rights-map` utility runs as a `root` user. Do not use GUI or CLI alternatively for mapping rights, it might cause issues with the assigned ACLs.

Syntax

```
user-rights-map -l
```

```
user-rights-map -L
```

```
user-rights-map -v <volume name> [[-u <User Map name 1 or the User Map 1
XML file path>,<User Map name 2 or the User Map 2 XML file path>,...,<User
Map name n or the User Map n XML file path> |-i <-U username -P
password>]][-a -m -r]
```

```
user-rights-map -S -M <map rights id> -O <ad | edir>
```

Options

-l, --list-map-rights

Lists the id, name of the user map, and the volume for which the rights are mapped.

-L, --list-usermaps

Lists the name of the user map, object mapping type (user to user, group to group, or container to group), eDirectory tree context, and Active Directory server context.

-v, --volume <*VOLUME_NAME*>

Specify the NSS volume on which rights will be provisioned for the mapped users. The volume name should always be specified in upper case.

-u, --usermap <*user map name or path of the user map xml file*>

Specify the name of the user map or the path of the user map (`.xml`) file that contains the mapping details of the eDirectory and Active Directory users, groups, or containers.

NOTE: If you need to perform a sync, you must pass the name of the user map as an input parameter. Whereas, if the sync operation is performed using the user map (`.xml`) file, it cannot be synced later.

-i, --use-IDM <-U *username* -P *password*>

Specify the eDirectory admin credentials (in LDAP format) to authenticate to eDirectory. The user map created using IDM is used for mapping the rights. This option is used only to create a rights map.

-a, --apply-to-salvage

Performs rights mapping on files and folders in the salvage system.

-m, --migrate-ids

Migrates the IDs [owner, archiver, metadata modifier, deletor] of files and folders to the mapped Active Directory users. This operation might take a while to complete.

-r, --remove-old-trustee

Removes the eDirectory user as a trustee on the files and folders after successfully mapping the user rights. Removes the Active Directory or eDirectory user as a trustee on the files and folders when used with -S, -O and -m options. This operation is irreversible.

-d, --delete-trustee

Deletes the eDirectory or Active Directory user as a trustee from the VIEW RIGHTS page, if the corresponding paired Active Directory or eDirectory trustee rights are removed on the selected path.

-S, --sync

Synchronizes the rights for both the eDirectory and Active Directory trustees. It is mandatory to use the sync option with the -M and -O options.

NOTE: The sync operation only synchronizes rights (applicable to salvage option). When creating the user map, if the options `migrate-ids` or `remove-old-trustee` are passed, they are ignored.

-M, --map-rights-id *<arg>*

Specify the id of the map rights operation. It also works with IDM rights map, but requires `-U` and `-P` options to provide eDirectory admin credentials. This option is used only with the sync option.

-O, --overwrite-with *<ad | edir>*

You must either pass `ad` or `edir` as an input parameter. When the `ad` parameter is passed, the rights of the eDirectory trustees are overwritten with the rights of the Active Directory trustees. When the `edir` is passed, the rights of the Active Directory trustees are overwritten with the rights of the eDirectory trustees. This option is used only with the sync option.

-h, --help

Displays the usage information of the command.

NOTE: The user rights map log information is located at `/var/opt/novell/log/nurm/userrights-map.log`.

Examples

1. Provision the rights on all files and folders of the volume MKTVOL, including the ones in the salvage system.

   ```
   user-rights-map -v MKTVOL -u /root/temp/UserMap.xml -a -m -r
   ```

   After successful execution of the user-rights-map operation, all the files and folders are provisioned with rights, all the ids are migrated, and the eDirectory user is removed as a trustee.

   NOTE: You can pass multiple user map names, multiple user map (xml) files, or both user map names and user map (xml) files as an input parameter (with comma separated). For example, `user-rights-map -v MKTVOL -u /root/temp/UserMap.xml,/root/temp/Map2.xml,usermap2 -a -m -r`.

   ---

2. To list the user maps:

   ```
   user-rights-map -L
   ```
   or
   ```
   user-rights-map --list-usermaps
   ```

3. To list the user rights map ids:

   ```
   user-rights-map -l
   ```
   or
   ```
   user-rights-map --list-map-rights
   ```

4. After the sync, the rights of the AD trustees are overwritten with the rights of eDirectory trustees. The rights of the Active Directory user2 are RWF and the rights of eDirectory user2 are FMA on file2:

   ```
   user-rights-map -S -M 11 -O edir -U cn=admin,o=novell -P novell
   ```

   After successful execution of the command, the rights of Active Directory user2 are FMA and the rights of eDirectory user2 are FMA on file2.

5. After the sync, the rights of the eDirectory trustees are overwritten with the rights of Active Directory trustees. The rights of the eDirectory user2 are RWF and the rights of Active Directory user2 are FMA on file2:

   ```
   user-rights-map -S -M 1 -O ad
   ```

   After successful execution of the command, the rights of eDirectory user2 are FMA and the rights of Active Directory user2 are FMA on file2.

6. To synchronize rights between eDirectory and AD trustees (two way sync):

   ```
   user-rights-map -S -M 2 -O edir -m -r
   ```

   Synchronizes the rights of eDirectory trustees with AD trustees using the map rights job id “2”. During the sync process, it overwrites the Active Directory trustees with eDirectory trustees, migrates all the IDs, and the eDirectory trustee information is removed from the source after the sync process.

   ```
   user-rights-map -S -M 2 -O ad -m -r
   ```

   Synchronizes the rights of AD trustees with eDirectory trustees using the map rights job id “2”. During the sync process, it overwrites the eDirectory trustees with AD trustees and migrates all the IDs, and the AD trustee information is removed from the source after the sync process.

7. To delete the rights of eDirectory or Active Directory trustees:

   ```
   user-rights-map -S -M 2 -O edir -d
   ```

   Deletes the rights of all eDirectory trustees (whose corresponding paired Active Directory trustee rights are removed) using the map rights job id “2”.

   ```
   user-rights-map -S -M 2 -O ad -d
   ```

   Deletes the rights of all Active Directory trustees (whose corresponding paired eDirectory trustee rights are removed) using the map rights job id “2”.

7.5 NFARM (OES File Access Rights Management)

OES File Access Rights Management (NFARM) is a shell (Windows) or finder (Mac) extension that enables eDirectory or Active Directory users on Windows and Mac workstation to perform Salvage and Purge operations. In addition,

- On Windows workstation, enables Windows Active Directory or eDirectory administrators or users to manage the access rights and quotas of AD or eDirectory users or groups on Storage Services (NSS) resources.
- On Mac workstation, enables Windows Active Directory or eDirectory administrators or users to manage the access rights and quotas of AD users or eDirectory users or groups on Storage Services (NSS) resources.

NFARM on Windows helps AD or eDirectory administrators or users with sufficient rights to manage the following:

- Trustees explicit rights, inherited rights filter, and view effective rights. You can also view trustees with rights from the selected path and child or parent directories.
- Owners, NSS attributes and directory quota
- User quotas

- All paths that a user is a trustee of
- Salvage and Purge

NOTE:

- For Active Directory, ensure the following:
  - User Quota and Files System Rights operations are restricted to AD domain administrators, and to use these features one should have logged in to the Windows workstation using the AD domain administrative credentials.
  - To view or modify User Quota and File System Rights for an AD user from the trusted domain or forest, ensure that the user belongs to AD supervisor group of the domain where OES server is joined.
- For eDirectory, ensure that the user is an administrator or with administrator equivalent rights.

The term object referred to in this section, indicates a path, folder, or volume.

After performing any operation in NFARM, you can click the following:

- **Apply** to save changes to the NSS file system and remain in the same window.
- **OK** to save changes to the NSS file system and exit.
- **Cancel** to discard changes and exit.

All these operations are performed on a Windows mapped network drive that is mapped to an NSS volume, NSS Folder, or CIFS Share in the Windows client. These shares must be compatible with OES 2015 or later servers that have NSS AD set up and configured.

Similarly, NFARM on Mac helps AD administrators eDirectory administrators or users with sufficient rights to manage the following:

- Trustees explicit rights, inherited rights filter, and view effective rights. You can also view trustees with rights from the selected path and child or parent directories.
- Owners, NSS attributes and directory quota
- User quotas
- Salvage and Purge (both AD or eDirectory users)

The term object referred to in this section, indicates a path, folder, or volume.

After performing any operation in NFARM, you can click the following:

- **Apply** to save changes to the NSS file system and remain in the same window.
- **Revert** to undo the changes and remain in the same window.
- **OK** to save changes to the NSS file system and exit.
- **Cancel** to discard changes and exit.

All these operations are performed on a OES mapped drive that is mapped to an NSS volume, NSS Folder, or CIFS Share in the Mac client.

This section includes the following:

- Section 7.5.1, “NFARM Support Matrix,” on page 85
- Section 7.5.2, “Prerequisites for Installing NFARM,” on page 85
- Section 7.5.3, “Installing and Accessing NFARM,” on page 86
- Section 7.5.4, “Managing the Trustee Rights in the NSS File System,” on page 86
- Section 7.5.5, “Information or Directory Quota,” on page 93
- Section 7.5.6, “User Quota,” on page 93
- Section 7.5.7, “File System Rights,” on page 95
- Section 7.5.8, “Settings (Mac),” on page 96
- Section 7.5.9, “Salvage and Purge,” on page 96
- Section 7.5.10, “Logs,” on page 97

7.5.1 NFARM Support Matrix

This section lists the requirements for installing and running NFARM:

- **Operating Systems:** NFARM can be installed on Windows and Mac:
  - **Windows (64-bit):** Windows 10
  - **Mac:** Mac OS X 10.15
- **OES:** NFARM for Mac is supported beginning with OES 2018.
- **Active Directory:** Active Directories installed and configured on Windows 2012 R2 and later.

7.5.2 Prerequisites for Installing NFARM

- Ensure that you have installed and configured NSS AD following the instruction at Chapter 4, “Installing and Configuring NSS AD Support,” on page 23.
- Ensure that the mapped network drive NSS volumes and CIFS shares are accessible. All NFARM operations are performed on a mapped network drive NSS volume or CIFS share that is compatible with OES 2015 or later servers that have NSS AD set up and configured. For more information on mapping a CIFS share, see “Accessing Files from a Windows Client” in the *OES 2023: OES CIFS for Linux Administration Guide*.
- Ensure that you have administrative rights on your workstation to install NFARM.
- Based on your operating system, download and install the correct version of NFARM from the OES Welcome page (https://*<OES server IP or the host name>*/welcome/client-software.html).
  - **Windows:** NFARM installer for Windows (64-bit)
  - **Mac:** NFARM installer for Mac

  NOTE: Beginning with OES 2018 SP2, NFARM on Mac does not support SMBv1 protocol.
- Ensure that your Windows operating system has been configured to authenticate using Active Directory.

- The maximum memory units that can be specified for the directory and user quotas in NFARM are as follows:
  - **KB:** 9007199254740991
  - **MB:** 8796093022207
  - **GB:** 8589934591
  - **TB:** 8388607
  - **PB:** 8191

7.5.3 Installing and Accessing NFARM

Based on your operating system, download the version of NFARM from the OES Welcome page (http://*<OES server IP Address or the host name>*/welcome/client-software.html) and install it.

After installing NFARM, map an NSS volume or CIFS share, and do the following to get access to NFARM tabs.

- **On Windows:** Right-click > **Properties** on the mapped share
- **On Mac:** Right-click > **Rights Management** on a OES mapped drive

  or

  To get access to only Salvage and Purge options, right-click > **Deleted Files** on a OES mapped drive.

On Windows workstation, when you map the volume for the first time as an eDirectory user and access any of the NFARM tabs, it prompts to enter the eDirectory credentials. The eDirectory user name should be in FQDN format. These credentials are used to list the eDirectory objects (only those objects for which the logged in eDirectory user has access to) in the eDirectory Object Selector window.

If there are a large number of trustees, the first launch of NFARM might fail to list them. The issue is caused because it takes time to fetch large number of trustees. Relaunch NFARM and the issue would be resolved because the trustees would be cached.

7.5.4 Managing the Trustee Rights in the NSS File System

On Windows

Using the Trustee Rights tab, you can do the following:

- View, add, edit, search, and remove trustees and their explicit rights on a selected path. The path can be the root of a volume, a folder in the volume, a file or a CIFS share.
- View both Active Directory and eDirectory trustees.
- View and edit the Inherited Rights Filter (IRF) for the selected path.
- View the effective rights trustees on the selected path, and manage the rights inheritance on the selected path.

Managing the Explicit Rights of Trustees

Explicit rights are the rights defined for the trustee (user or group) on an object. The trustee names are displayed in FQDN (for eDirectory user or group) and it is preceded by the AD domain name (for AD user or group) along with the following eight NSS rights:

- **Supervisor:** Grants all rights to the directory or file and any subordinate items. The Supervisor right can't be blocked by an Inherited Rights Filter. Users with this right can grant or deny other users rights to the directory or file.
- **Read:** For a directory, grants the right to open files in the directory and read the contents or run the programs. For a file, grants the right to open and read the file.
- **Write:** For a directory, grants the right to open and change the contents of files in the directory. For a file, grants the right to open and write to the file.
- **Erase:** Grants the right to delete the directory or file.
- **Create:** For a directory, grants the right to create new files and directories in the directory. For a file, grants the right to create a file and to salvage a file after it has been deleted.
- **Modify:** Grants the right to change the attributes or name of the directory or file, but does not grant the right to change its contents (changing the contents requires the Write right).
- **File Scan:** Grants the right to view directory and file names in the file system structure, including the directory structure from that file to the root directory.
- **Access Control:** Grants the right to add and remove trustees for directories and files and modify their trustee assignments and Inherited Rights Filters.

  This right does not allow the trustee to add or remove the Supervisor right for any user. Also, it does not allow to remove the trustee with the Supervisor right.

NOTE: These NSS rights are not related to the Microsoft Windows rights in any way.

This section explains the procedure to add, remove, or search trustees on an object, in addition to managing their explicit rights on the selected object:

- To add trustees on a selected path:
  - When you map the volume as an AD user, click **Add...**, search and select the AD users or groups, then select the rights. If you are entering multiple trustee names in the **Enter the object names to select (examples)** text box, separate each trustee with a semicolon.
  - When you map the volume as an eDirectory user, click **Add...**. Specify the object name, search context, select the object type, and then click **Search**. In the User or Group Name list, select the eDirectory user or group and click **OK**.
  - When you map the volume as an eDirectory user, then to add AD trustees, select **List Active Directory trustees also**, and click **Add**. In Identify Source dialogue box, select Active Directory and click **OK**. Similarly, when you map the volume as an AD user, then you can add eDirectory trustees too.
- To remove trustees, select the trustees that you want to remove, then click **Remove**.

TIP: To delete multiple trustees, press and hold the Ctrl key while selecting multiple trustees.

- To search for a specific trustee in the trustee list, specify the trustee name, and click **Search**. To revert to the original trustee list, clear the entry in the search box, and then click **Search**.

- To edit or remove rights for the displayed trustees, select or clear the respective rights check boxes. Multiple trustee edit is possible.
- To list the eDirectory and Active Directory trustees in the trustee list, select **List Active Directory trustees also**, or **List eDirectory trustees also**. After listing, you can continue to perform a search, add or remove trustees, edit or remove rights.

After managing the explicit rights, ensure that you click **Apply** in order for your changes take effect in the NSS file system.

Managing Inherited Rights Filter (IRF)

Subdirectories and files can inherit rights from their parent directory. The directory's rights flow down through its structure to subdirectories and files, except for specific subdirectories or files with their own trustee assignments that supersede inherited rights. When granting a trustee assignment to a subdirectory or file, the trustee assignment takes precedence over the inherited rights of its parent directory.

The Inherited Rights Filter section displays the list of rights that are inherited from the parent object. To block inheritance of rights from the parent object to the selected object (file or directory), clear the respective NSS rights, then click **Apply** for the changes to take effect in the NSS file system.

The supervisor rights cannot be blocked.

Viewing the Effective Rights

A user's explicit rights on a directory are combined with the filtered rights inherited from its parent directory. Any rights through security equivalence are also applied.

A user's explicit rights on a file override any rights that can be inherited from its parent directory. In this case, the user has only the rights granted, and the inherited rights are ignored. If the user is a member of another group or role that also has explicit rights to the file, the user's effective rights on the file are a combination of the rights granted for the user and the rights granted for the group or role. If the rights of the group or role are more restrictive than the user's explicit rights, it has no effect on rights granted to the user.

An object's effective rights to a subdirectory are the set of distinct rights from the following:

- Rights inherited for the user from the parent directory, with consideration of the inherited rights filter set for the subdirectory.
- Rights set explicitly for the user on the directory.
- Rights set explicitly for a security-equivalent object on the directory:
  - Explicit by assignment (Security Equal To property)
  - Automatic by membership in a group or role
  - Implied by its parent container and by the [Public] container

  More restrictive security-equivalent rights do not override rights granted for the trustee on the directory or for the trustee's filtered inherited rights.

An object's effective rights to a file are determined by the following:

- Rights inherited for the user from the parent directory, with consideration of the inherited rights filter set for the file.

If the user has rights set on the parent directory or is security equivalent to an object with explicit rights set there, those are the rights that flow down to the file for the user and are subject to the IRF.

Inherited rights for a file are ignored if rights are set explicitly for the object or for a security equivalent of the object. This behavior is different than for a directory.

- Rights set explicitly for the user on the file.

  Inherited rights are ignored. Explicit trustee rights for a security equivalent object are added. More restrictive security-equivalent rights do not override rights set for the trustee on the file.
- Rights set explicitly for a security-equivalent object on the file:
  - Explicit by assignment (Security Equal To property)
  - Automatic by membership in a group or role
  - Implied by its parent container and by the [Public] container

    Inherited rights are ignored. Explicit trustee rights are added.

For more information, see How Effective Rights Are Calculated in the NetIQ eDirectory Administration Guide.

To launch the Effective Rights screen, from the Trustee Rights tab, click **Advanced...**. By default, for the selected object, the list of trustees along with their rights is displayed. You can use the **Search** button to view the rights of a specific trustee in the trustee list.

NOTE: To revert to the original trustee list, clear the entry in the search box, and then click **Search**.

To view the effective rights of some other trustee, click **Select**:

- When you map the volume as an AD user, search or enter the trustee name.
- When you map the volume as an eDirectory user, search the trustee name in the **User or Group Name** list, select the eDirectory user or group, and then click **OK**. You can select only one user at a time.

You must have adequate rights to view the effective rights of other trustees.

Managing Trustees for Directories

Using the Trustees for Directories tab, you can get the explicit rights of the trustees from the selected path to the root of the volume and trustees from the selected path to the child directories in the volume.

To launch the Trustees for Directories screen, from the Trustee Rights tab, click **Advanced... > Trustees for Directories**.

For example, assume that you have the following directory structure:

- \vol1\media\audio
- \vol1\org\country\us\ny\emp
- \vol1\org\country\us\slc\emp
- \vol1\org\country\uk\ln\emp
- \vol1\org\country\uk\lpl\emp

If you click **Parent Directories** from the “country” folder, it will list the explicit list of trustees and their rights in the country, org and vol1. It does not consider the media and its sub directories.

If you click **Sub Directories** from the countries folder, it lists the explicit rights of all the trustees in the following directories:

- \vol1\org\country\us\
- \vol1\org\country\us\ny
- \vol1\org\country\us\slc
- \vol1\org\country\us\ny\emp
- \vol1\org\country\us\slc\emp
- \vol1\org\country\uk
- \vol1\org\country\uk\ln
- \vol1\org\country\uk\lpl
- \vol1\org\country\uk\ln\emp
- \vol1\org\country\uk\lpl\emp

From this tab, you can also modify the explicit rights of the trustees by clearing or selecting the NSS rights check boxes. You can also remove trustees by using the **Remove** button. To search for a specific trustee in the trustee list, specify the trustee name, and click **Search**.

NOTE: To revert to the original trustee list, clear the entry in the search box, and then click **Search**.

On Mac

Using the Trustee Rights tab, you can do the following:

- View, add, edit, search, and remove trustees and their explicit rights on a selected path. The path can be the root of a volume, a folder in the volume, a file or a CIFS share.
- View and edit the Inherited Rights Filter (IRF) for the selected path.
- View the effective rights trustees on the selected path, and manage the rights inheritance on the selected path.

Managing the Explicit Rights of Trustees

Explicit rights are the rights defined for the trustee (user or group) on an object. The trustee names are displayed in FQDN (for eDirectory user, group, or container) and it is preceded by the AD domain name (for AD user or group) along with the eight NSS rights. For more information on these eight rights, see “Managing the Explicit Rights of Trustees” on page 87 on Windows.

This section explains the procedure to add, remove, or search trustees on an object, in addition to managing their explicit rights on the selected object:

- To add trustees on a selected path, click , search and select the users or groups, then select the rights.

NOTE: In the Settings tab, if you have enabled the option List eDirectory trustees also or List Active Directory trustees also, then an additional pop-up is displayed to select the identity source.

- To remove trustees, select the trustees that you want to remove, then click −.

TIP: ◆**To select all files:** Select the first file, then press COMMAND+A.

- **To select multiple files:** Press and hold the ALT key, then click the files of your choice..
- **To select a series of files:** Select the first file, press and hold the SHIFT key, and then click the last file.

- To search for a specific trustee in the trustee list, specify the trustee name in the search box.
- To edit or remove rights for the displayed trustees, select or clear the respective rights check boxes. Multiple trustee edit is possible.
- To list the eDirectory and Active Directory trustees in the trustee list, select List both eDirectory and AD trustees. After listing, you can continue to perform a search, remove trustees, edit or remove rights, but you cannot add any user to the trustee list.

After managing the explicit rights, ensure that you click **Apply** in order for your changes take effect in the NSS file system or click **Revert** to undo the changes.

Managing Inherited Rights Filter (IRF)

Subdirectories and files can inherit rights from their parent directory. The directory's rights flow down through its structure to subdirectories and files, except for specific subdirectories or files with their own trustee assignments that supersede inherited rights. When granting a trustee assignment to a subdirectory or file, the trustee assignment takes precedence over the inherited rights of its parent directory.

The Inherited Rights Filter section displays the list of rights that are inherited from the parent object. To block inheritance of rights from the parent object to the selected object (file or directory), clear the respective NSS rights, then click **Apply** for the changes to take effect in the NSS file system or click **Revert** to undo the changes.

The supervisor rights cannot be blocked.

Viewing the Effective Rights

A user's explicit rights on a directory are combined with the filtered rights inherited from its parent directory. Any rights through security equivalence are also applied.

A user's explicit rights on a file override any rights that can be inherited from its parent directory. In this case, the user has only the rights granted, and the inherited rights are ignored. If the user is a member of another group or role that also has explicit rights to the file, the user's effective rights on the file are a combination of the rights granted for the user and the rights granted for the group or role. If the rights of the group or role are more restrictive than the user's explicit rights, it has no effect on rights granted to the user. For more information on effective rights, see "Viewing the Effective Rights" on page 88 on Windows.

By default, for the selected object, the list of trustees along with their rights is displayed. You can use the **Search** button to view the rights of a specific trustee in the trustee list.

To view the effective rights of some other trustee, click **Select**, then search or enter the trustee name.

NOTE: If you enable the List both **eDirectory** and **AD trustees** option on the Rights tab, you cannot view the effective rights of other trustees.

You must have adequate rights to view the effective rights of other trustees.

Managing Trustees for Directories

Using the Trustee for Directories tab, you can get the explicit rights of the trustees from the selected path to the root of the volume and trustees from the selected path to the child directories in the volume.

For example, assume that you have the following directory structure:

- \vol1\media\audio
- \vol1\org\country\us\ny\emp
- \vol1\org\country\us\slc\emp
- \vol1\org\country\uk\ln\emp
- \vol1\org\country\uk\lpl\emp

If you click **Parent Directories** from the “country” folder, it will list the explicit list of trustees and their rights in the country, org and vol1. It does not consider the media and its sub directories.

If you click **Sub Directories** from the countries folder, it lists the explicit rights of all the trustees in the following directories:

- \vol1\org\country\us\
- \vol1\org\country\us\ny
- \vol1\org\country\us\slc
- \vol1\org\country\us\ny\emp
- \vol1\org\country\us\slc\emp
- \vol1\org\country\uk
- \vol1\org\country\uk\ln
- \vol1\org\country\uk\lpl
- \vol1\org\country\uk\ln\emp
- \vol1\org\country\uk\lpl\emp

From this tab, you can also modify the explicit rights of the trustees by clearing or selecting the NSS rights check boxes. You can also remove trustees by using the button. To search for a specific trustee in the trustee list, specify the trustee name in the search box.

7.5.5 Information or Directory Quota

On Windows

Using the Information tab, you can view and modify:

- The owner of a file
- NSS attributes
- Directory quotas

1. To change the owner of a file, click **Change**, then search for and select the new owner.
2. To set the NSS attributes for the selected path, select or clear the respective attributes. These attributes vary based on the object chosen (file or directory).
3. To change the directory quota of a selected path, click **Edit**, then specify the quota limit and the memory unit (KB, MB, GB, TB, PB). After setting the quota, you will be able to view the quota limit set, the used quota and the available quota.
4. Click **Apply** for the changes to take effect in the NSS file system.

On Mac

Using the Directory Quota tab, you can view and modify:

- The owner of a file
- NSS attributes
- Directory quotas

1. To change the owner of a file, click , then search for and select the new owner.

   NOTE: In the Settings tab, if you have enabled the option List eDirectory trustees also or List Active Directory trustees also, then an additional pop-up is displayed to select the identity source.

   ---

2. To set the NSS attributes for the selected path, select or clear the respective attributes. These attributes vary based on the object chosen (file or directory).
3. To change the directory quota of a selected path, click , then specify the quota limit and the memory unit (MB, GB, TB, PB). After setting the quota, you will be able to view the quota limit set, the used quota and the available quota.
4. Click **Revert** to undo the changes or click **Apply** for the changes to take effect in the NSS file system.

7.5.6 User Quota

Using the User Quota tab, you can add, edit, or remove the user quota limit for a single or multiple users concurrently. For every user, it lists the quota limit, used, and remaining.

On Windows

To set the user quota:

- For Active Directory users, you should either be an AD domain administrator or a user who has administrative privileges. You should also be logged in to the Windows workstation using the AD domain administrative credentials.
- For eDirectory users, you should either be an eDirectory administrator or a user who has administrative privileges.

To search for a specific trustee in the trustee list, specify the trustee name, and click **Search**. To revert to the original trustee list, clear the entry in the search box, and then click **Search**.

1. To assign quotas for a single or multiple users, click **Add**..., search and select users, then specify the quota limit.
2. To edit the quota limit, select users, click **Edit**..., then modify the quota limit. Press and hold the Ctrl key while selecting multiple users.
3. To remove the quota set for users, select the users, then click **Remove**.

NOTE: The user quota is always set at the volume level, regardless of the folder or share from where you have invoked the User Quota.

On Mac

To set the user quota:

- For Active Directory users, you should either be an AD domain administrator or a user who has administrative privileges. You should also be logged in to the Windows workstation using the AD domain administrative credentials.
- For eDirectory users, you should either be an eDirectory administrator or a user who has administrative privileges.

1. To assign quotas for a single or multiple users, click . A new window is displayed, click , search and select users, then specify the quota limit.

   NOTE: In the Settings tab, if you have enabled the option List eDirectory trustees also or List Active Directory trustees also, then an additional pop-up is displayed to select the identity source.

   ---

2. To edit the quota limit, select users, click , then modify the quota limit and click **Ok**. Press and hold the Alt key while selecting multiple users.
3. To remove the quota set for users, select the users, then click .
4. Click **Revert** to undo the changes or click **Apply** for the changes to take effect in the NSS file system.

NOTE: The user quota is always set at the volume level, regardless of the folder or share from where you have invoked the User Quota.

7.5.7 File System Rights

On Windows

Using the File System Rights tab, you can do the following:

- View all the objects that a user is a trustee of
- Modify the explicit rights that the trustee has on an object
- Add or remove the objects
- View the rights of all groups to which the user is a member

---

NOTE: To view or modify the File System Rights:

- For Active Directory users, you should either be an AD domain administrator or a user who has administrative privileges. Further, you should have logged in to the Windows workstation using the AD administrative credentials.
- For eDirectory users, you should either be an eDirectory administrator or a user who has administrative privileges.

---

1. To view the explicit rights of a trustee across objects at the volume level, click **Select**, then search and select a user or group.

   NOTE: If you enable the List both eDirectory and AD trustees option on the Trustee Rights tab, you cannot select any user or group name to view the explicit rights of a trustee.

   ---

2. To modify the explicit rights that the trustee has on an object, select or clear the respective NSS rights check boxes next to the object name.
3. To add an object and to assign rights to the trustee, click **Add...**, then select the path.
4. To remove an object on which the trustee has rights, select the object, then click **Remove**. Press and hold the Ctrl key while selecting multiple objects.
5. To view rights of all the groups to which the trustee belongs, click **Group Rights**. Group Rights is disabled if a group is selected.

On Mac

Using the File System Rights tab, you can do the following:

- View all the objects that a user is a trustee of
- Modify the explicit rights that the trustee has on an object
- Add or remove the objects
- View the rights of all groups to which the user is a member

NOTE: To view or modify the File System Rights:

- For Active Directory users, you should either be an AD domain administrator or a user who has administrative privileges. Further, you should have logged in to the Mac workstation using the AD administrative credentials.
- For eDirectory users, you should either be an eDirectory administrator or a user who has administrative privileges.

1. To view the explicit rights of a trustee across objects at the volume level, click ,then search and select an user or a group.

   NOTE: In the Settings tab, if you have enabled the option List eDirectory trustees also or List Active Directory trustees also, then an additional pop-up is displayed to select the identity source.

2. To modify the explicit rights that the trustee has on an object, select or clear the respective NSS rights check boxes next to the object name.
3. To add an object and to assign rights to the trustee, click **Add or remove path**, select the object, then assign rights and click **Apply**.
4. To remove an object on which the trustee has rights, select the object, then click **Add or remove path**. Press and hold the Ctrl key while selecting multiple objects.
5. To view the rights of all the groups to which the trustee belongs, click **Group Rights**. **Group Rights** is disabled if a group is selected.
6. Click **Revert** to undo the changes or click **Apply** for the changes to take effect in the NSS file system.

7.5.8 Settings (Mac)

Using the Settings tab, you can enable the ability to manage trustees from both eDirectory and Active Directory across all the tabs.

To enable managing the trustees from both Active Directory and eDirectory, select the checkbox **List Active Directory trustees also** or **List eDirectory trustees also**.

7.5.9 Salvage and Purge

The Salvage and Purge utility lets you recover or delete the files and directories permanently from the NSS file system. The files that have been purged cannot be recovered. This tool gets automatically installed when you install NFARM.

For information on how to perform salvage and purge operations on Windows, see Salvage and Purge on Windows in the OES 2023: OES CIFS for Linux Administration Guide.

For information on how to perform salvage and purge operations on Mac, see Salvage and Purge on Mac in the OES 2023: OES CIFS for Linux Administration Guide.

7.5.10 Logs

On Mac

- Application log location - `/Users/<username>/Library/Logs/nfarm/<application_name>.log`
- Crash Reports - `/Users/<username>/Library/Logs/DiagnosticReports/`
- Run-time logs - `Launch Console.app`

On Windows

Log location - `C:\Users\<username>\AppData\Roaming\NFARM`

7.6 FTP (Pure-FTPd) and OES for AD Users

FTP file services on OES servers are provided by Pure-FTPd, a free (BSD), secure, production-quality and standard-conformant FTP server. The OES implementation includes support for FTP gateway functionality as on OES and offers a level of integration between AD and Pure-FTP that allows users to authenticate to AD for FTP access to the server.

This section discusses the following topics:

- Section 7.6.1, “Planning for Pure-FTPd,” on page 97
- Section 7.6.2, “Installing Pure-FTPd,” on page 97
- Section 7.6.3, “Home Directory Support in Pure-FTPd,” on page 98
- Section 7.6.4, “Prerequisites,” on page 99
- Section 7.6.5, “Configuring Pure-FTPd on an OES Server,” on page 99
- Section 7.6.6, “Administering and Managing Pure-FTPd on an OES Server,” on page 99
- Section 7.6.7, “SMB Access for AD Users,” on page 102
- Section 7.6.8, “Limitations,” on page 102

7.6.1 Planning for Pure-FTPd

Before installing Pure-FTPd, ensure that users requiring FTP access have access rights to the areas on the server they need to use.

7.6.2 Installing Pure-FTPd

To install Pure-FTPd, select the **OES FTP** pattern in the OES installation.

7.6.3 Home Directory Support in Pure-FTPd

The FTP server supports a home directory for users on local and remote CIFS servers. The remote server should be an OES server. When the home directory is set for the user in AD, the user is placed in the home directory on successful login to the OES server.

Pure-FTPd supports three levels of home directory, default home directory, a user specific home directory on the local system, and a user specific home directory identified by the value set in AD.

DefaultHomeDirectory or AD home directories can be disabled. If both of them are enabled, the following is used to establish the precedence:

- User specific home directory set in AD
- Default home directory

User Specific Home Directory in AD

An administrator can set the home directory for AD users as part of the User object in AD. On successful login to the FTP server, the user is placed in the home directory set in the user object. The User's home directory can exist either on the OES server that is hosting the FTP service or on any other OES server in the same tree.

A new `EnableRemoteHomeDirectory` option is now available to support this home directory. By default, this option is set to *NO* and the home directory set for the user in AD is ignored.

To enable AD based home directory support, you must set both `EnableRemoteHomeDirectory` and `remote_server` to YES. FTP will then read the user's home directory from AD and mount it locally.

Default Home Directory

DefaultHomeDirectory indicates the path to the common home directory for all FTP users. On successful login to the Pure-FTPd, users are placed in the default home directory. The default home directory can be a locally mounted NSS path or on a remote CIFS share. The NSS volume can be configured by using the `DefaultHomeDirectory` and `DefaultHomeDirectoryServer` settings. If the home directory is on a remote server, use `DefaultHomeDirectoryServer`, and set the DNS name of the remote CIFS server. As with any NSS volume, the FTP client should have required rights over the NSS volume whether DefaultHomeDirectory is on a local or remote server or not.

The `DefaultHomeDirectoryServer` option is now available to differentiate whether DefaultHomeDirectory is on a local or remote server. By default, this option is set to *NO* so DefaultHomeDirectory points to a local path.

To set `DefaultHomeDirectory` to point to a remote CIFS server with a DNS entry, you must specify the full path to the remote server, including the share name. For example, `DefaultHomeDirectory /sharename.` You must also set both `DefaultHomeDirectory` and `remote_server` to YES.

NOTE: The following are not supported for AD users:

- POSIX home directory
- Trusted GID feature

Backslash in Input Paths

Support for backslashes in input path is provided. Using FTP client on Windows, you can use backslash as separator in the path. `allow_backslash_in_path` option is now available to allow back slash in the path. By default the option is set to NO.

7.6.4 Prerequisites

Ensure that the FTP server can resolve the DNS name of the remote OES server.

7.6.5 Configuring Pure-FTPd on an OES Server

To configure the Pure-FTPd server on OES, edit the `/etc/pure-ftpd/pure-ftpd.conf` file.

NOTE: It is very strongly recommended that you read through the entire `/etc/pure-ftpd/pure-ftpd.conf` file and be familiar with the available parameters and settings.

For more information, see the `pure-ftpd` man page.

7.6.6 Administering and Managing Pure-FTPd on an OES Server

- "Starting Pure-FTPd" on page 99
- "Initializing Multiple Instances" on page 99
- "Unloading Specific Instances" on page 100
- "Pure-FTPd Remote Server Navigation" on page 101

Starting Pure-FTPd

Start the Pure-FTPd server using the `rcpure-ftpd` command.

Initializing Multiple Instances

Pure-FTPd is loaded by using a configuration file. Multiple instances of Pure-FTPd can be loaded using different configuration files.

By default, an instance of Pure-FTPd using `/etc/pure-ftpd/pure-ftpd.conf` file is loaded at the boot time. For loading multiple instances, new configuration files need to be created.

To load a new instance of Pure-FTPd:

1. Create a new configuration file for each instance.

   For example: Copy `/etc/pure-ftpd/pure-ftpd.conf` to `/etc/opt/novell/pure-ftpd1.conf`.

2 Modify the following settings in the configuration file to avoid IP address or port conflicts between the instances:

- **PIDFile:** Points to the full path of the PID file created by the pure-ftpd instance. PID file is used for unloading a particular instance of pure-ftpd. Hence, ensure that the PID File path is unique for every instance.

  For example: `/var/run/pure-ftp1.pid`, `/var/run/pure-ftp2.pid`.

- **Bind:** By default, pure-ftpd binds to all the IP addresses on the system and listens to requests over port 21. Modify the settings of the bind such that all the pure-ftpd instances bind to different IP addresses or port combinations.

  also, modify the settings in the `/etc/pure-ftpd/pure-ftpd.conf` to avoid any IP address or port conflict from the second instance.

  For example: If a system has two interfaces with two IP addresses 10.1.1.1 and 10.1.1.2, then the bind setting for two pure-ftpd instances can be *Bind 10.1.1.1,21* and *Bind 10.1.1.2,21*.

3 Load the new instance using `/usr/sbin/pure-config.pl <Full path of the config file>`

For example: `/usr/sbin/pure-config.pl /etc/opt/novell/pureftpd-confs/pure-ftpd1.conf` loads an instance using the config file `/etc/opt/novell/pureftpd-confs/pure-ftpd1.conf`.

Verifying the Load of a New Instance

Use the following methods to verify that the new instance of pure-ftpd is successfully loaded:

- The `ps –eaf | grep pure-ftpd` command lists all the instances of pure-ftpd loaded on the system.
- The PID file as specified using the `PIDFile` entry in the configuration file has been created.
- An FTP connection from the client to the server over the IP address being used by the pure-ftpd instance can be created.

Unloading Specific Instances

A new script, `pure-ftp-stop.pl`, is added to unload an instance of pure-ftpd and all its child processes. The full path of the configuration file used to load the instance of pure-ftpd must be passed to the `pure-ftp-stop.pl` script.

For example: `/usr/sbin/pure-ftpd-stop.pl /etc/opt/novell/pureftpd-confs/pure-ftpd1.conf` unloads the instance of pure-ftpd that was loaded using `/etc/opt/novell/pureftpd-confs/pure-ftp1.conf`.

The PID file of the pure-ftpd instance is also used for unloading the pure-ftpd instance.

Verifying the Unload of a New Instance

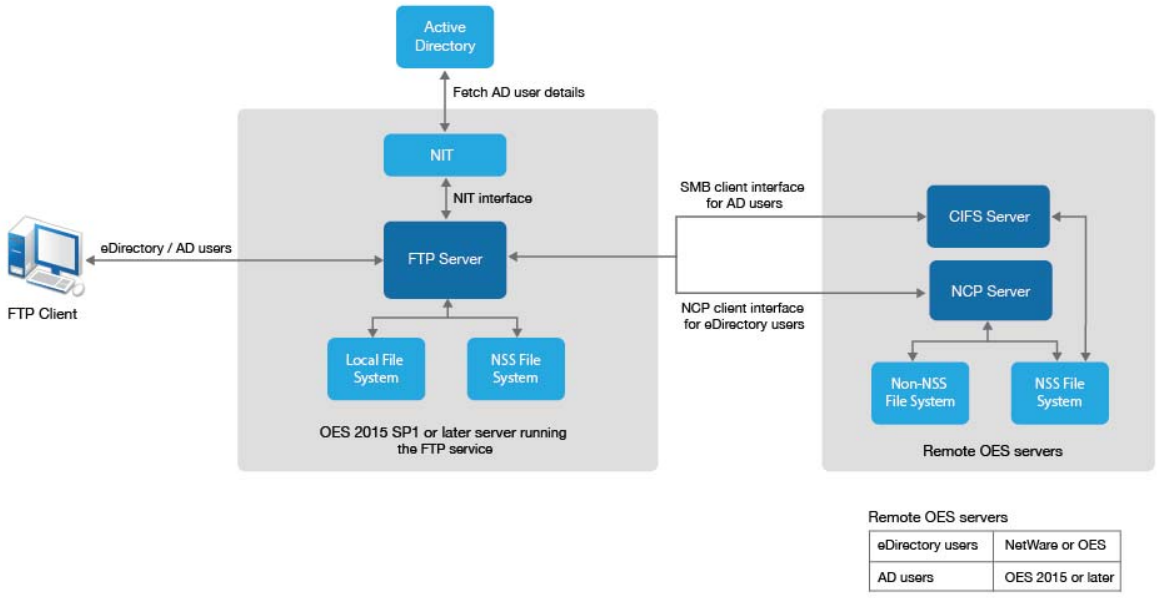
- The PID file specified using the `PIDFile` entry in the configuration file has been deleted.
- The number of instances displayed by `ps –eaf | grep pure-ftpd` is reduced.
- An FTP connection request to the server errors out.

Pure-FTPd Remote Server Navigation

After logging in to the AD tree, users can access files and directories on a remote Linux server whether or not the server is running Linux FTP Server software. The remote server can be another Linux OES server.

This section describes how to configure and use the Remote Server Navigation feature.

- "Configuring OES FTP" on page 101
- "Path Formats" on page 102



Remote OES servers

eDirectory users	NetWare or OES
AD users	OES 2015 or later

The CIFS protocol lets you transfer files and navigate to and from remote OES servers.

To navigate to remote servers, use the following command:

```
cd //remote server name/share/directory pathname
```

File operations such as `get`, `put`, and `delete` can be used on the remote server, even without changing the directory path to that server.

For example:

```
get //remote_server_name/share/directory path/filename
```

The double slash (//) indicates that the user wants to access a remote server. After the double slash, the first entry must be the name of the remote server. The remote server name should be full DNS server name.

Configuring OES FTP

Configuration file: /etc/pure-ftpd/pure-ftpd.conf

The configuration parameters for remote server navigation are as follows:

Entry	Value	Function
remote_server	yes	Enables remote server navigation for the Pure-FTPd server.

The following configuration parameters needs to be set for remote server navigation:

Entry	Value	Reason Why
ChrootEveryone	no	Option yes restricts users to login only to his home directory and cannot navigate to other directories including remote OES servers.
AnonymousOnly	no	Option yes allows only anonymous login.
NoRename	no	Option yes restricts users to rename the file.

Path Formats

Table 7-3 *Linux FTP Server path formats*

Task	Command Format
Specifying the volume and directory path name	//server_name/share_name/directory_path
Navigating to different volumes	cd //server_name/share_name
Switching back to the home directory	cd ~
Switching to the root of the server	/root

NOTE: ◆The Linux FTP Server does not support wildcards at the root of the server.

- When chroot capability is enabled, AD users are allowed to login with chrooted.

7.6.7 SMB Access for AD Users

By default, AD users access files through SMB protocol. Beginning with OES 2018 SP1, they can also access files through SMB2 protocol. To enable this, add the entry `client max protocol = SMB2` under the 'global' heading in `/etc/samba/smb.conf` on the FTP server.

```
[global]
client max protocol = SMB2
```

Enabling SMB2 access for AD users provides them the capability to access DFS junctions.

7.6.8 Limitations

Co-existence Issue in Default Home Directory for Cluster Volumes: If Default Home Directory is used and the physical and cluster pool names is greater than 15 characters, then the NCP and CIFS server names will be different. Therefore, FTP login is impacted for both Remote Home Directory and Default Home Directory.

If eDirectory and Active Directory users co-existence is needed, run two instances of FTP server. One instance for eDirectory users with NCP (Virtual) server name and another instance for Active Directory users with CIFS (netbios) server name. For more information on initializing multiple instances, see “Initializing Multiple Instances” on page 99.

8 Troubleshooting

This section presents information on troubleshooting the NSS AD installation and configuration.

- Section 8.1, “OES Storage Services AD Configuration is Greyed Out,” on page 105
- Section 8.2, “Domain Leave Fails Using the novell-ad-util,” on page 105
- Section 8.3, “Verification of the Container Object Fails During the AD Domain Join Process,” on page 106
- Section 8.4, “Troubleshooting NFARM on MAC,” on page 106
- Section 8.5, “Troubleshooting NURM,” on page 107
- Section 8.6, “Troubleshooting NIT,” on page 108

8.1 OES Storage Services AD Configuration is Greyed Out

The OES Storage Services AD configuration is already done and if you try to reconfigure the same in the YaST screen, the OES Storage Services AD configuration is greyed out. This is because the keytab entries are not empty and results in domain leave failure.

To resolve this issue, ensure that the domain leave is successful. For more information, see “Verifying the Domain Leave” on page 46.

8.2 Domain Leave Fails Using the novell-ad-util

After verifying the steps provided in “Verifying the Domain Leave” on page 46, the domain leave still fails. This is because,

- Domain Controller (DC) or DNS server is not working properly or
- Netbios name of the OES host or cluster resource is modified after the OES host or cluster resource is joined to the AD domain.

To resolve this issue, perform the following:

1. Delete the computer objects in the AD domain manually.
2. Remove the `/etc/krb5.keytab` file.
3. In case of cluster resource, remove the `/media/nss/VOL1/._NETWARE/vol.keytab` file.

After completing these steps, the OES host and cluster resource are brought back to the state where it can be joined to the AD domain.

8.3 Verification of the Container Object Fails During the AD Domain Join Process

“Error: Verification of container object failed. Ensure that the AD Server is reachable.”

If you encounter the above error during the AD domain join process, ensure that you have set the following:

- AD server's reverse lookup entry (IPv4 and IPv6) in the DNS server before the domain join operation is performed.
- AD domain name to which the OES server will be joined to as part of the Domain Search in OES server network settings.

8.4 Troubleshooting NFARM on MAC

- Section 8.4.1, “'Rights Management' Menu Not Available,” on page 106
- Section 8.4.2, “Unable to view Trustees in the Trustee Rights or User Quotas Tab,” on page 106
- Section 8.4.3, “Connection to Active Directory Failed,” on page 106
- Section 8.4.4, “NFARM Terminated Unexpectedly,” on page 107

8.4.1 'Rights Management' Menu Not Available

To resolve this issue:

1. Click System **Preferences** > **Extensions**.
2. Verify the new extensions - `FileRightsInfo` and `SalvagePurge` are available under the **All** option.
3. Ensure the `Finder` extensions are enabled.

8.4.2 Unable to view Trustees in the Trustee Rights or User Quotas Tab

To resolve this issue:

1. Save the credential of the server in the Keychain and relaunch the finder.

   NFARM uses mapped-in user’s credential stored in keychain to interact with the OES server.

8.4.3 Connection to Active Directory Failed

Issues:

- Connection to the AD server failed.
- Unable to view the Users or Groups in the AD browser

Solution:

Verify the AD connections.

For example - **Directory Utility** > **Directory Editor** > **Select "/Active Directory/<ad domain name>"** in nodes. Should list all the users.

8.4.4 NFARM Terminated Unexpectedly

If the NFARM application crashes, unmount the `IPC$` and `_admin` volumes (if its exists) and restart the application.

To restart the Finder in Mac:

- Go to **Apple Menu > Force Quit > Finder** and then click **Relaunch**.

To verify, execute the command `df -h`

For example,

- `umount –f /Volumes/IPC$`
- `umount –f /Volumes/_admin`

8.5 Troubleshooting NURM

- Section 8.5.1, "Unable to Map eDirectory Users in NURM," on page 107
- Section 8.5.2, "Volumes are not Listed in the View Rights and Map Rights Pages," on page 108
- Section 8.5.3, "Active Directory User Names With Special Characters are Ignored," on page 108
- Section 8.5.4, "View Rights Option Does Not Work in NURM When There are 200K Users," on page 108

8.5.1 Unable to Map eDirectory Users in NURM

User mapping fails if the organization unit (ou) name in NURM contains the following special characters:

```
\ % # / ; , < > ?
```

However, the following special characters in ou name will not result in any user mapping failure:

```
}{[] | _-  "': !@$^&*()
```

8.5.2 Volumes are not Listed in the View Rights and Map Rights Pages

NURM uses CIFS to fetch the volume information. The volumes do not get listed in the View Rights and Map Rights pages under the following conditions:

- When a user who is not universal password enabled accesses NURM, the volumes do not get listed under the View Rights and Map Rights pages. To resolve this issue, ensure to set the Universal Password Policy for the user who is accessing NURM. For more information on enabling Universal Password Policy, see CIFS and Universal Password in the OES 2023: OES CIFS for Linux Administration Guide.

- When the CIFS user context is not configured for the eDirectory user who is accessing NURM. For more information, see Configuring a CIFS User Context in the OES 2023: OES CIFS for Linux Administration Guide.
- When the user, who is accessing NURM, does not have adequate rights on `/_admin/Manage_NSS/manage.cmd`.

8.5.3 Active Directory User Names With Special Characters are Ignored

While creating a user in AD, if it contains any special characters (/\[]:;|=,+*?<>@"), it is replaced with an underscore (_) in the SAM account name after a warning; whereas, the user name continues to have the special character. For example, if you want to create a user named "tom*adm", the SAM account name will be "tom_adm", and the user name will be "tom*adm".

When you use IDM to synchronize the identity sources (eDirectory and Active Directory), IDM creates a user in eDirectory with the name "tom*adm". In this scenario, if you use NURM to map and apply rights, it ignores the identities with special characters.

8.5.4 View Rights Option Does Not Work in NURM When There are 200K Users

"Error: Error in Communication."

When you try to view the rights of 200,000+ users, NURM displays the error as mentioned above. This happens due to Java memory issues.

To increase the Java memory:

1. Edit `/etc/opt/novell/tomcat/conf/novell-tomcat.conf` and update the JAVA_OPTS entry as follows:

   ```
   JAVA_OPTS="-Djava.library.path=/opt/novell/eDirectory/lib64:/var/opt/novell/tomcat/lib:/usr/lib64 -Xms1024m -Xmx2048m"
   ```

2. Restart the OES instance of tomcat using the `rcnovell-tomcat restart`.

8.6 Troubleshooting NIT

- “Unspecified GSS failure. Minor code may provide more information (Ticket expired)” on page 109
- “Invalid UID Obtained” on page 109
- “Unable to fetch tree name, error:11” on page 109

Unspecified GSS failure. Minor code may provide more information (Ticket expired)

Description: Ticket Granting Ticket (TGT) expiration errors are seen if the NIT setting `ad-tgt-refresh-timeout` is more than the "Maximum lifetime for a user ticket" in the Kerberos policy of the domain.

Action: To avoid TGT expiration errors, ensure that the `ad-tgt-refresh-timeout` value is less than Active Directory TGT expiration time.

Invalid UID Obtained

Description: If the Active Directory user is denied access possibly the user is not assigned a valid UID.

Cause: Run the `nitconfig get` command and check if `ad-uid-generate-mode` parameter is set to 0. Setting this parameter to 0 means NIT operates in Fetch mode for Active Directory users and tries to fetch UIDs for those users from Active Directory. If the users do not have UIDs assigned in Active Directory you might encounter this error.

Action: When you choose to fetch UID for Active Directory users, NIT fetches the `uidNumber` attribute set in Active Directory for all the Active Directory users. If UID is not set for a particular user, that user cannot access NSS file systems. If you are configuring NIT in fetch mode for Active Directory users, ensure that the Active Directory users who require access to NSS filesystems have UID numbers set in the Active Directory. Add the uidNumber attribute explicitly to the Global Catalog server as it is not part of default attributes. For more information about replicating UID numbers to the Global Catalog server, refer to the Microsoft Support website.

Unable to fetch tree name, error:11

Description: eDirectory is down and NIT is not able to fetch tree name.

Action:

1. Start eDirectory by running the `rcndsd start` command.
2. Start NIT by running the `rcnovell-nit start` command

A Reference Information

- Section A.1, “NIT Error Codes,” on page 111

A.1 NIT Error Codes

0	NIT_SUCCESS	Success
-9001	NITERR_ENTRY_NOTFOUND	Active Directory search returned unexpected results.
-9002	NITERR_ATTRIBUTE_NOTFOUND	Specified attribute is not found in the Active Directory. For example: SID, UID, GUID and so on.
-9003	NITERR_UIDRANGE_EXHAUSTED	The UID range has been exhausted.
-9004	NITERR_IO_ERROR	Unable to write the NIT configuration file.
-9005	NITERR_PERMISSION_DENIED	Request comes from a non-root user, permission is denied to perform the operation.
-9006	NITERR_NITD_UNAVAILABLE	NIT daemon is not running.
-9007	NITERR_AD_LDAP_TIMEOUT	NIT did not receive an answer from the LDAP server before the timeout interval.
-9008	NITERR_EDIR_ONLY_MODE	NIT runs in eDirectory mode, cannot perform Active Directory search operations.
-9009	NITERR_INSUFFICIENT_BUFFER	The caller has not allocated enough memory.
-9010	NITERR_INSUFFICIENT_MEMORY	There is no enough memory to allocate.
-9011	NITERR_UNKNOWN_ERROR	Cause is unknown.
-9012	NITERR_NO_USER_ACCESS_GROUP	Active Directory universal access group **OESAccessGrp** is not found.
-9013	NITERR_MANY_USER_ACCESS_GROUP	More than one Active Directory license universal group is found.
-9014	NITERR_INVALID_PARAMETER	The parameters passed are NULL or invalid.
-9015	NITERR_INVALID_SUPERVISOR_GROUP	Specified Active Directory supervisor group is not valid.
-9016	NITERR_AD_NOT_REACHABLE	Active Directory server is not reachable.
-9017	NITERR_EDIR_NOT_REACHABLE	eDirectory server is not reachable.